# Virtual Private Network Capability Package

National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

# VIRTUAL PRIVATE NETWORK CAPABILITY PACKAGE

This Commercial Solutions for Classified (CSfC) Capability Package describes how to protect classified data in transit across an untrusted network using a virtual private network (VPN) implemented with multiple layers of Internet Protocol Security (IPsec) encryption.

**Version 3.2**
**August 20, 2015**

## CHANGE HISTORY

| Title | Version | Date | Change Summary |
|---|---|---|---|
| Commercial Solutions for Classified (CSfC) Multi-Site Virtual Private Network (VPN) Capability Package | 0.8 | March 14, 2012 | • Initial release of CSfC Virtual Private Network (VPN) guidance. |
| Commercial Solutions for Classified (CSfC) Multi-Site Virtual Private Network (VPN) Capability Package | 1.0 | August 17, 2012 | • Official release of CSfC VPN guidance.<br>• Adjudicated public review of Multi-Site VPN CP 0.8. |
| Commercial Solutions for Classified (CSfC) Virtual Private Network (VPN) Capability Package | 1.08 | March 4, 2013 | • Initial release of CSfC VPN guidance for remote access.<br>• Added Remote Access capability and associated requirements and test procedures.<br>• Split compound requirements into separate requirements.<br>• Assigned requirement identifiers to "shall" statements in Sections 4 and 5 of Multi-Site VPN CP 1.0.<br>• Explicitly identified which requirements apply to each capability.<br>• Explicitly identified threshold and objective requirements. |
| Commercial Solutions for Classified (CSfC) Virtual Private Network (VPN) Capability Package | 2.0 | May 28, 2013 | • Official release of CSfC VPN guidance.<br>• Added requirements for using a single VPN solution for networks of multiple security levels.<br>• Added use cases for End User Devices (EUDs) in non-remote-access scenarios.<br>• Split and renumbered compound requirements. |
| Commercial Solutions for Classified (CSfC) Virtual Private Network (VPN) Capability Package | 2.08 | December 19, 2013 | • Initial release of CSfC VPN guidance for use of a single Gray network with networks of multiple security levels.<br>• Initial release of CSfC VPN guidance for distribution of Certificate Revocation Lists (CRLs) on the external side of VPN Gateways.<br>• Added additional requirements for the content and distribution of CRLs. |

# Virtual Private Network Capability Package

| Title | Version | Date | Change Summary |
|---|---|---|---|
| Commercial Solutions for Classified (CSfC) Virtual Private Network (VPN) Capability Package | 3.0 | July 22, 2014 | • Official release of CSfC VPN guidance for use of a single Gray network with networks of multiple security levels.<br>• Official release of CSfC VPN guidance for distribution of CRLs on the external side of VPN Gateways.<br>• Introduced new manufacturer diversity, device management, and incident reporting requirements.<br>• Clarified Threshold and Objective requirement relationships. |
| Commercial Solutions for Classified (CSfC) Virtual Private Network (VPN) Capability Package | 3.1 | March 11, 2015 | • Corrected error in VPN-PF-11<br>• Corrected error in Section 14.15<br>• Changed VPN-DM-19 from T=O to O<br>• Changed VPN-DM-20 from T=O to O |
| Commercial Solutions for Classified (CSfC) Virtual Private Network (VPN) Capability Package | 3.2 | August 20, 2015 | • Removed all references to EUDs from this capability package.<br>• Added new Cryptography standards in accordance with CNSSP 15. |

## TABLE OF CONTENTS

## TABLE OF FIGURES



## TABLE OF TABLES

# 1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) program within the National Security Agency (NSA) Information Assurance Directorate (IAD) uses a series of Capability Packages to provide configurations that will allow customers to independently implement secure solutions using layered Commercial Off-the-Shelf (COTS) products. The Capability Packages are vendor-agnostic and provide high-level security and configuration guidance for customers and/or Solution Integrators.

IAD is delivering a generic CSfC Virtual Private Network (VPN) Capability Package to meet the demand for data in transit solutions using a secure sharing suite (S3) of algorithms. These algorithms, known as Suite B algorithms, are used to protect classified data using layers of COTS products. VPN Capability Package Version 3.2 enables customers to implement VPNs between two or more sites. This Capability Package takes lessons learned from multiple proof-of-concept demonstrations that had implemented a set of S3 algorithms, modes of operation, standards, and protocols. These demonstrations included a layered use of COTS products for the protection of classified information.

This document, the CSfC VPN Capability Package Version 3.2, clarifies the intent s for the direction of the CSfC VPN Capability Package. It offers additional flexibility in creating a single VPN solution that supports multiple classified networks (see Section 4.3.2.2) and in the distribution of certificate status information to solution components (see Section 4.3.3). These new capabilities are intended to reduce the implementation and management costs of large-scale VPN solutions that comply with this Capability Package.

VPN solutions that had been designed to comply with the CSfC VPN Capability Package Version 3.1 dated, 11 March 2015, which contained End User Devices (EUDs) will no longer be supported by this Capability Package. Customers requiring client remote access will need to register their solutions against the Mobile Access v1.1 Capability Package. Appendix D provides a detailed summary of the differences between Version 3.1 and Version 3.2 of the CSfC VPN Capability Package.

This document, the CSfC VPN Capability Package Version 3.2, supersedes the previously released CSfC VPN Capability Package Version 3.1 dated March 11, 2015.

# 2 PURPOSE OF THIS DOCUMENT

This Capability Package provides high-level reference designs and corresponding configuration information that allows customers to select COTS products from the CSfC Components List, available on the CSfC web page (http://www.nsa.gov/ia/programs/csfc_program), for their VPN solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data while in transit. As described in Section 9, customers must ensure that the components selected from the CSfC Components List will permit the necessary functionality for the selected capabilities. To successfully implement a solution based on this Capability Package, all Threshold requirements, or the

corresponding Objective requirements applicable to the selected capabilities, must be implemented, as described in Section 8.

Customers who want to use the solution detailed in this Capability Package must contact NSA to determine ways to obtain NSA approval. Additional information about the CSfC process is available on the CSfC web page (www.nsa.gov/ia/programs/csfc_program).

# 3 USE OF THIS DOCUMENT

This document, the CSfC VPN Capability Package Version 3.2, dated August 20, 2015, has been approved by the IAD Director and will be reviewed twice a year to ensure that the defined capabilities and other instructions still provide the security services and robustness required. Solutions designed according to this Capability Package must be registered with NSA/IAD. Once registered, a signed IAD Approval Letter (see sample in Appendix D) will be sent validating that the VPN solution is registered as a CSfC solution, validated to meet the requirements of the latest VPN Capability Package, and is approved to protect classified information. Any solution designed according to this Capability Package may be used for one year and must then be revalidated against the most recently published version of the Capability Package.

Please provide comments on usability, applicability, and/or shortcomings to your NSA/IAD Client Advocate and the VPN Capability Package maintenance team at vpn@nsa.gov.

The following Legal Disclaimer relates to the use of this Capability Package:

This Capability Package is provided “as is.” Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the United States Government be liable for any direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data, or profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this Capability Package, even if advised of the possibility of such damage.

The User of this Capability Package agrees to hold harmless and indemnify the United States Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorney’s fees, court costs, and expenses, arising in direct consequence of Recipient’s use of the item, including, but not limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights.

Nothing in this Capability Package is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer’s product or service.

# 4 DESCRIPTION OF THE VPN SOLUTION

This Capability Package describes a general VPN solution to protect classified information as it travels across either an untrusted network or a network of a different classification level. The solution supports interconnecting two or more networks operating at the same security level via a VPN, where the security level encompasses the classification level, list of compartments, dissemination controls, and other such controls over information. The solution provides sufficient flexibility to be applicable to many use cases of VPN implementations.

The VPN solution uses two nested, independent Internet Protocol Security (IPsec) tunnels to protect the confidentiality and integrity of data as it transits the untrusted network. The two IPsec tunnels protecting a data flow are generated by VPN Gateways implemented as part of the network infrastructure.

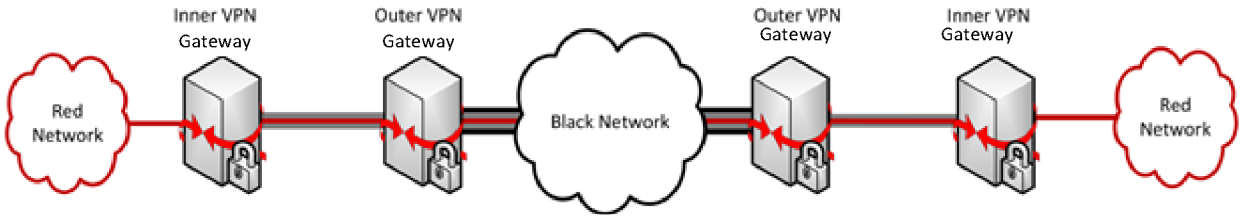


**Figure 1. Two IPsec Tunnels Protect Data across an Untrusted Network**

As shown in Figure 1, before being sent across the untrusted network, each packet of classified data is encrypted twice: first by an Inner VPN Gateway, and then by an Outer VPN Gateway. At the other end of the data flow, the received packet is correspondingly decrypted twice: first by an Outer VPN Gateway, and then by an Inner VPN Gateway.

## 4.1 NETWORKS

This Capability Package uses the following terminology to describe the various networks that comprise a VPN solution and the types of traffic present on each.

### 4.1.1 RED, GRAY, AND BLACK

The terms Red, Gray, and Black identify the type of encryption, if any, that has been applied to classified data within a single network.

A Red network contains unencrypted classified data and is logically located behind an Inner VPN Gateway. The networks connected to one another through the VPN solution are each Red networks. Red networks are under the control of the solution owner or a trusted third party. Red networks may only communicate with one another through the VPN solution if the networks operate at the same security level.

A Gray network contains classified data that has been encrypted once. The network between an Inner VPN Gateway and an Outer VPN Gateway is a Gray network. Gray networks are under the control of the solution owner or a trusted third party. A VPN solution compliant with this Capability Package treats Gray networks as unclassified networks, albeit subject to unique security requirements. If a solution owner's classification authority determines that a Gray network itself is classified, perhaps by determining the Internet Protocol (IP) addresses used on Gray network interfaces are classified at some level, then the VPN solution described in this Capability Package cannot be implemented, as it is not designed to ensure that such information will be afforded two layers of protection.

A Black network contains classified data that has been encrypted twice. The network connecting the Outer VPN Gateways together is a Black network. Black networks are not necessarily (and often will not be) under the control of the solution owner, and may be operated by an untrusted third party.

### 4.1.2 Data, Management, and Control Plane Traffic

Data plane traffic is the actual classified information, encrypted or not, that is being passed through the VPN solution. The VPN solution exists to encrypt and decrypt data plane traffic. All data plane traffic within the Gray and Black networks is encapsulated within the ESP protocol.

Management plane traffic is used to configure and monitor solution components. It includes the communications between a system administrator and a component, as well as the logs and other status information forwarded from a solution component to a log server or similar repository. All management plane traffic on Red and Gray networks is encapsulated within the SSHv2, ESP, or TLS protocol.

Control plane traffic consists of other protocols necessary for the network to function that carry neither data nor management traffic. Control plane traffic is typically not initiated directly on behalf of a user (unlike data traffic) or a system administrator (unlike management traffic). Many, but not all, control plane protocols operate at Layer 2 or Layer 3 of the Open Systems Interconnection (OSI) model. Examples of control plane traffic include, but are not limited to, the following:

- Network address configuration (e.g. DHCP, NDP, etc.)
- Address resolution (e.g. ARP, NDP, etc.)
- Name resolution (e.g. DNS, etc.)
- Time synchronization (e.g. NTP, PTP, etc.)
- Route advertisement (e.g. RIP, OSPF, IS-IS, BGP, etc.)
- IPsec session establishment (i.e. IKEv1, IKEv2)
- Certificate status distribution (e.g. OCSP, HTTP download of CRLs, etc.)

In general, this Capability Package does not impose detailed requirements dealing with control plane traffic, although control plane protocols may be used in order to implement certain requirements. For example, requirements VPN-SR-4 and VPN-SR-5 (see Section 10.1) require that time synchronization be performed, but do not require the use of any particular time synchronization protocol or technique. Notable exceptions are for IPsec session establishment and for certain certificate status distribution scenarios (see Section 4.3.3) where, given their impact on the security of the solution, this Capability Package does provide detailed requirements. Unless otherwise specified in this Capability Package, the usage of specific control plane protocols is left to the solution owner to approve, but any control plane protocols not approved by the solution owner should be disabled.

Data plane and management plane traffic are generally required to be separated from one another by using separate LANs or VLANs for each (see Section 10.7, requirements VPN-DM-4 and VPN-DM-5). As a result, a solution may, for example, have a Gray Data network and a Gray Management network which are separate from one another, where the components on the Gray Management network are used to manage the components on the Gray Data network. Given that some control plane traffic is necessary for a network to function, there is no general requirement that control plane traffic be similarly separated, unless otherwise specified.

## 4.2 INTEROPERABILITY

The VPN solution defined in this Capability Package supports interoperability by having similar standards-based configurations at both ends of each layer of the solution. However, there is no guarantee of generic interoperability between any two products on the CSfC Components List. An IAD goal is to create and realize adoption of IPsec implementation standards that will allow for this generic interoperability in the future.

## 4.3 HIGH-LEVEL DESIGN

The VPN solution is adaptable to support capabilities for multiple sites and/or multiple security levels, depending on the needs of the customer implementing the solution. If a customer does not have a need for supporting multiple sites or multiple security levels, then those elements need not be included as part of the implementation. However, any implementation of the VPN solution must satisfy all of the applicable requirements specified in this Capability Package, as explained in Section 8.

### 4.3.1 MULTIPLE SITES

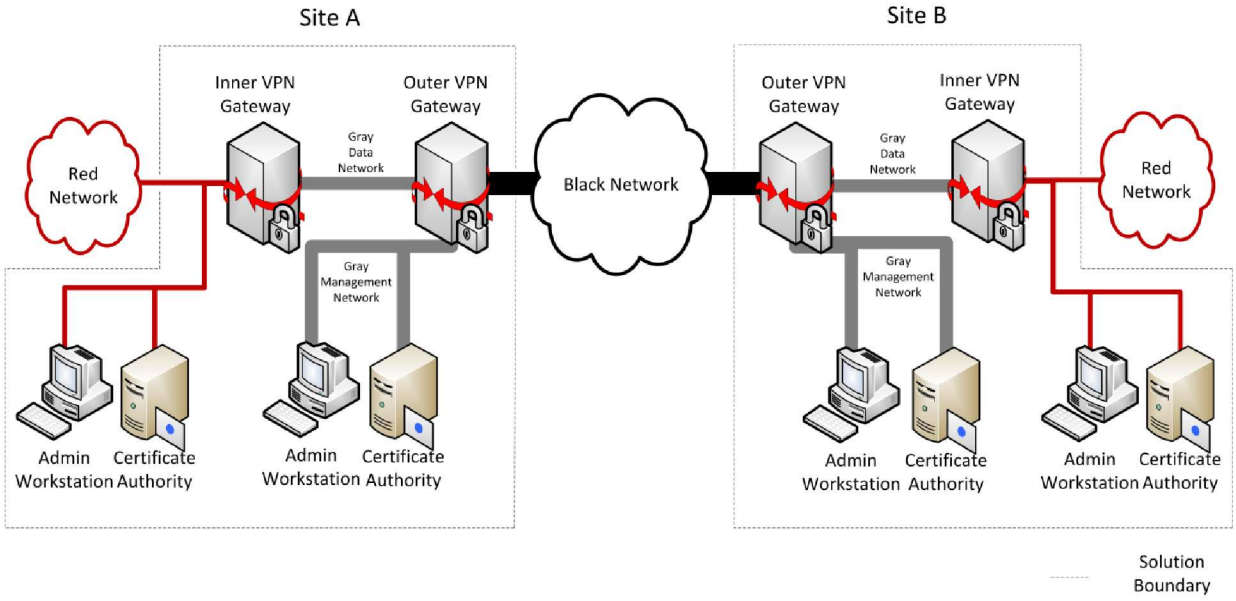


**Figure 2. VPN Solution Connecting Two Independently Managed Sites**

Figure 2 depicts two Red networks at different sites that operate at the same security level, connected to one another through the VPN solution. Here, each Red network has two VPN Gateways associated with it: an Inner VPN Gateway connected to the Red network, and an Outer VPN Gateway between the Inner VPN Gateway and the Black network. There are two layers of IPsec tunneling between any pair of sites communicating directly with one another: one IPsec tunnel between their Outer VPN Gateways, and a second IPsec tunnel between their Inner VPN Gateways.

There is no limit to the number of sites that may be incorporated into a single VPN solution.

Sites in the solution may be managed independently of one another, or may be remotely managed from a central site.

#### *4.3.1.1 Independently Managed Sites*

For independently managed sites, each site performs the administration of its own VPN Gateways and has the option of using either locally-run Certificate Authorities (CAs) that they manage and control (see Figure 2) or, where available, enterprise CAs which are not necessarily managed by the solution owner. Each site needs to ensure that the VPN Gateways selected interoperate with those at the other sites. In addition, the two VPN Gateways at each site need to have the signing certificates and revocation information for the corresponding CAs used by the other sites in the VPN solution. Since there is no remote management, no management traffic will cross the Black network, encrypted or otherwise.

This high-level design requires cooperation between the various sites in the solution to ensure that all CAs used by each site are trusted at all the other sites. This model has the advantage of allowing

communication between larger organizations that have a need to share information while maintaining independence.

Note that while Figure 2 depicts only two sites, this solution can scale to include numerous sites, with each additional site having the same design as those in the figure.

#### *4.3.1.2 Centrally Managed Sites*

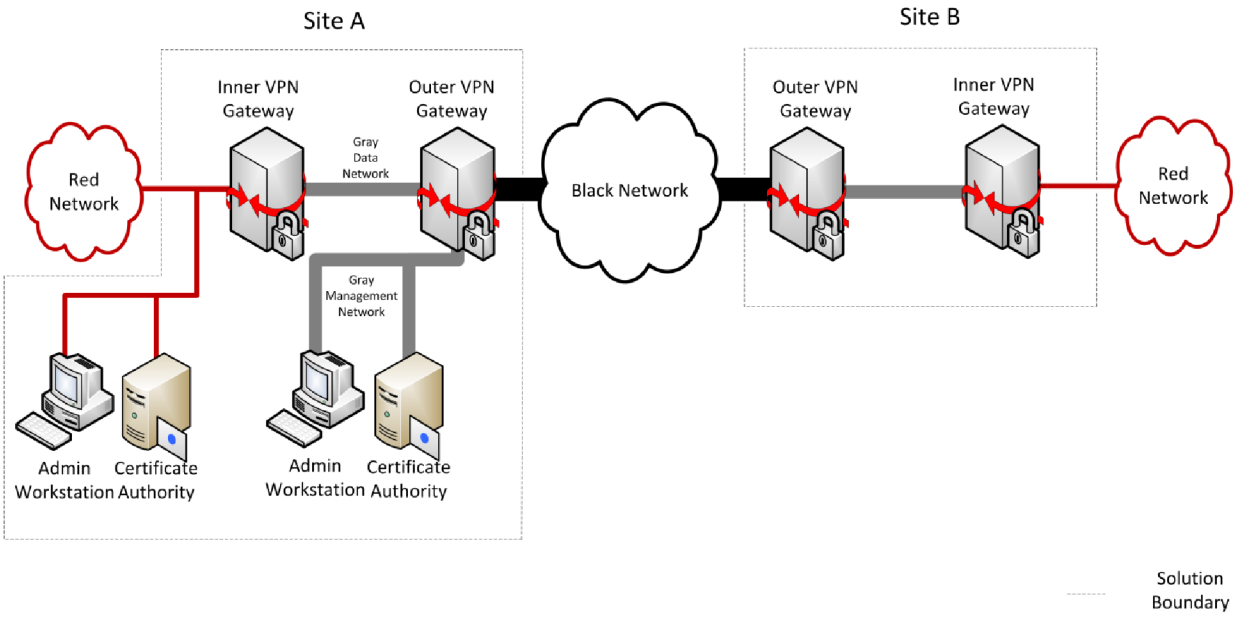


**Figure 3. VPN Solution Connecting a Central Management Site and a Remote Site**

If remote management is used, personnel at a single geographic site administer and perform keying for all the various sites included in the solution, as shown in Figure 3. In this case, because the administration is done by one group of Security Administrators and CA Administrators (see Section 12), they can ensure the interoperability of each site as new sites are added. Only two CAs are needed: one on the Red network for all the Inner VPN Gateways and one on the Gray Management network for all the Outer VPN Gateways. If available, enterprise CAs should be used.

Because the central management site manages the VPN Gateways at the other sites over the network, encryption is used to logically separate data and management traffic as it passes between sites. Gray management traffic is encrypted using Secure Shell version 2 (SSHv2), Transport Layer Security (TLS), or IPsec before being routed through the Outer VPN Gateway to another site. The SSHv2, TLS, or IPsec serves as the inner layer of encryption for Gray management traffic, and the IPsec tunnel handled by the Outer VPN Gateway serves as the outer layer of encryption. Red management traffic is similarly encrypted before being routed through the Inner and Outer VPN Gateways to another site. As a result, all management traffic between sites is encrypted at least twice before transiting the Black network.

This model makes it easier to add sites because of the centralized administration.

Note that while Figure 3 depicts only two sites, this solution can scale to include numerous sites, with each additional site having the same high-level design as the remotely managed site in the figure.

### 4.3.2 Multiple Security Levels

A single implementation of the VPN solution may support Red networks of different security levels. The VPN solution provides secure connectivity between the Red networks within each security level while preventing Red networks of differing security levels from communicating with one another. This enables a customer to use the same physical infrastructure to carry traffic from multiple networks. Although each Red network will still require its own Inner VPN Gateway, a site may use a single Outer VPN Gateway to encrypt and transport traffic that had been encrypted by Inner VPN Gateways of varying security levels.

There is no limit to the number of different security levels that a VPN solution may support.

VPN solutions supporting multiple security levels may include independently managed sites (see Section 4.3.1.1) or centrally managed sites (see Section 4.3.1.2). Given both cases, separate CAs and management devices are needed to manage the Inner VPN Gateways at each security level. For example, Figure 3 depicts a Central Management Site and a Remote Site, but Network 1 and Network 2 each have their own CA and management devices, which prevent their Inner VPN Gateways from being able to authenticate with one another.

#### *4.3.2.1 Same Classification Level*

For Red networks that operate at the same classification level but different security levels, the cryptographic separation provided by the Inner VPN Gateways is sufficient to protect against unintended data flows between security levels. Two Inner VPN Gateways for networks of different classification levels will be unable to mutually authenticate with each other because they trust different CAs which do not have a trust relationship with one another. This prevents the establishment of an IPsec tunnel between the two components.

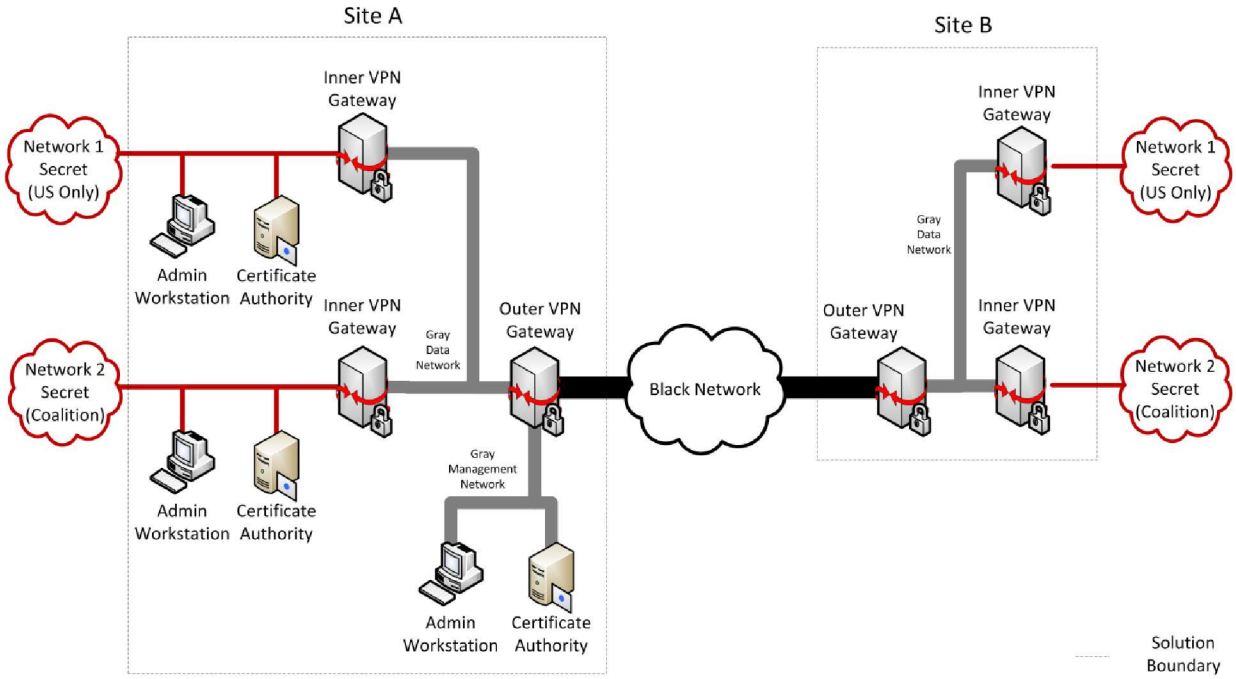


**Figure 4.VPN Solution for Two Networks of the Same Classification Level**

Figure 4 illustrates a VPN solution between two sites that carries traffic between two Red networks: a Secret U.S.-only network (Network 1) and a Secret coalition network (Network 2). Because Network 1 and Network 2 both operate at the Secret classification level, their singly-encrypted traffic can be carried over the Gray network without any additional security controls in place.

Although not required by this Capability Package, a solution owner may choose to implement the additional security described in Section 4.3.2.2 to provide additional protection against unintended data flows between Red networks at the same classification level.

#### *4.3.2.2 Different Classification Levels*

For Red networks of different classification levels, the cryptographic separation of their traffic on a Gray network, as described in Section 4.3.2.1, is still present. However, because the consequences of an unintended data flow between different classification levels are more severe than of one within a single classification level, an additional mechanism is necessary to further guard against such a flow from occurring.

This Capability Package uses packet filtering within Gray networks as an additional mechanism to prevent data flows between networks of different classification levels. Any physical path through a Gray network between a pair of Inner VPN Gateways supporting Red networks of different classification levels must include at least one filtering component. This filtering component restricts the traffic flowing through it based primarily on the Gray network source and destination addresses, only allowing a packet

through if the source and destination components are intended to communicate with one another and dropping the packet if they are not.

Additionally, filtering components are included between the components used for management of the Gray Networks themselves (namely, Administration Workstations and locally-run CAs) and Inner VPN Gateways that support Red networks of a lower classification level than the highest-classification Red network supported by the solution. In other words, Administration Workstations and locally-run CAs on Gray networks are treated as and grouped with the Inner VPN Gateways with the highest-classification Red network.

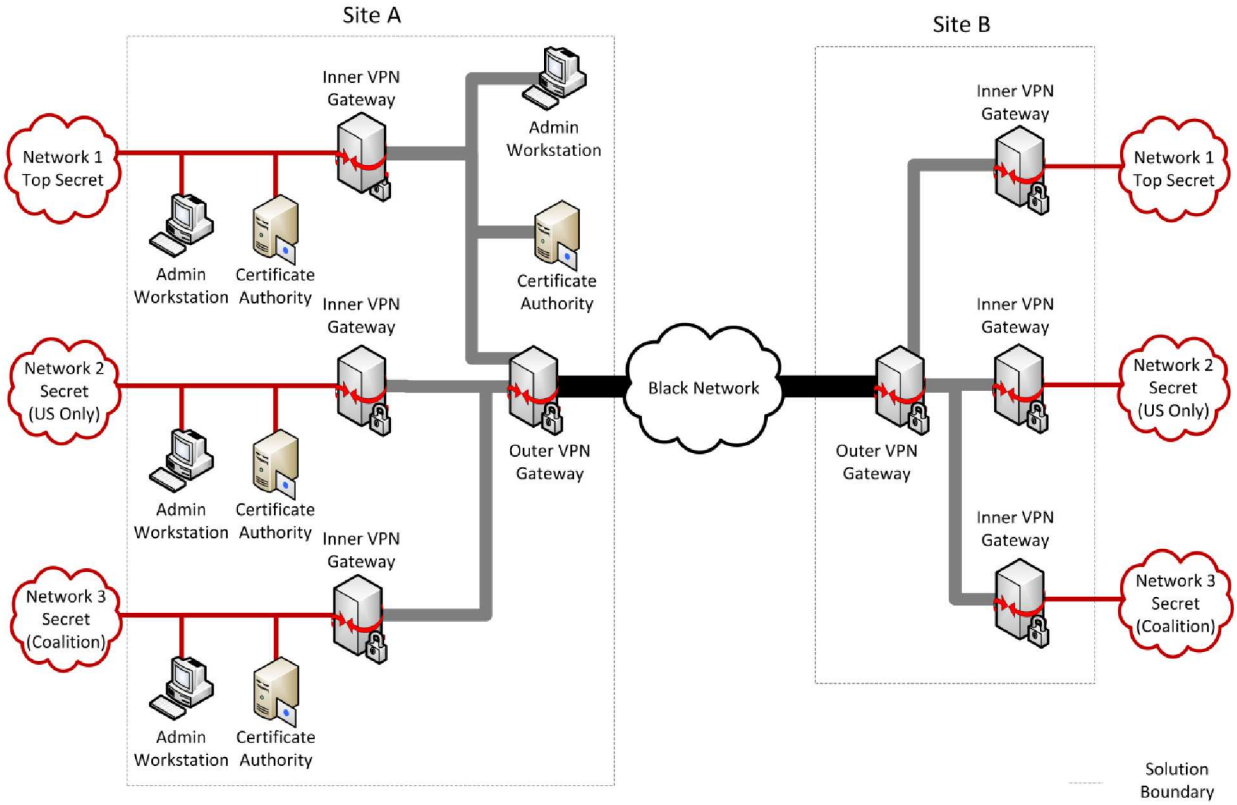


**Figure 5. Using Outer VPN Gateways for Gray Network Filtering**

This Capability Package provides some flexibility in where this filtering takes place within the Gray network. The simplest option is to implement the filtering on the Outer VPN Gateways, as shown in Figure 5. Here, the VPN solution is supporting three Red networks: one Top Secret network (Network 1) and two Secret networks (Networks 2 and 3). Any path through the Gray network between an Inner VPN Gateway for a Secret network and an Inner VPN Gateway for the Top Secret network (or for the Gray Network's Administration Workstation or CA) includes at least one Outer VPN Gateway, which performs the filtering function. Effectively, the Gray network at each site is split into two separate networks which

only meet at the Outer VPN Gateway: one supporting the Secret networks, and one supporting the Top Secret network (and Gray Network management).

Note that there is no filtering component on the path between the Inner VPN Gateways for Network 2 and Network 3 within each site, but this is acceptable because Networks 2 and 3 operate at the same classification level; see Section 4.3.2.1 for more details.

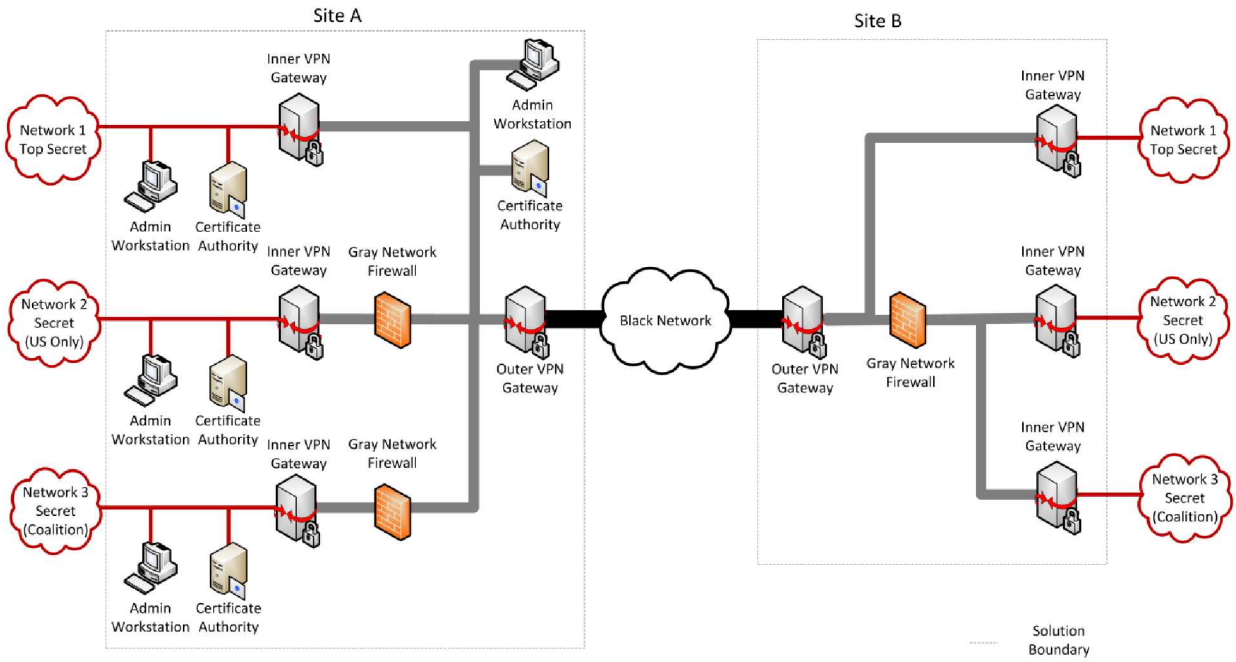


**Figure 6. Using Standalone Gray Network Firewalls for Gray Network Filtering**

However, some solutions may be subject to physical constraints that prevent relying exclusively on the Outer VPN Gateways to provide the filtering function. To accommodate these situations one or more Gray Network Firewalls can be included in a Gray network to perform the filtering in addition to the Outer VPN Gateways, as shown in Figure 6. Here, the Gray network is laid out in such a way that the paths between any two Inner VPN Gateways within the same site do not pass through an Outer VPN Gateway. Instead, standalone Gray Network Firewalls have been placed at each site between the Inner VPN Gateways for the Secret networks and the rest of the Gray network; these Gray Network Firewalls are responsible for dropping any packets between an Inner VPN Gateway for Network 1 and an Inner VPN Gateway for Network 2 or 3.

Figure 6 also illustrates that there is flexibility in the specific placement of Gray Network Firewalls, as long as their placement satisfies the requirement that any path between Inner VPN Gateways for networks of different classification levels is met. Site A and Site B in the figure demonstrate two possible placements of Gray Network Firewalls that would satisfy this requirement, although other acceptable placements are also possible.

Including one or more standalone Gray Network Firewalls in a solution does not remove the requirement to perform the filtering on the Outer VPN Gateways as well. Outer VPN Gateways are uniquely positioned to block traffic between Inner VPN Gateways supporting Red networks of different classification levels when one of those Inner VPN Gateways is located at a different site.

### 4.3.3 External Distribution of Certificate Revocation Lists

Part of the security of the VPN solution depends on the certificate-based mutual authentication that occurs between two VPN Gateways establishing a VPN tunnel. One step of this mutual authentication entails checking whether the certificate used by the other VPN Gateway has been revoked, which requires each VPN Gateway to have access to a current Certificate Revocation List (CRL). As the number of sites interconnected through the VPN solution increases, out-of-band CRL distribution becomes increasingly burdensome and error-prone. Although VPN Gateways may retrieve the latest CRL directly from the appropriate CA, for Remote Sites this requires first establishing a VPN connection to the Central Management Site where the CAs are located. These additional VPN connections increase the time needed to establish a VPN connection between two Remote Sites. Furthermore, the Remote Site's VPN Gateways still require out-of-band CRL distribution in order to be able to check for revocation of the certificates used by VPN Gateways at the Central Management Site, since the VPN connection to the Central Management Site must be established before the CRLs can be obtained from the CAs.

To avoid these issues, this Capability Package permits the distribution of CRLs on the external side of the VPN Gateways, which allows the VPN Gateways to retrieve the current CRL without first establishing a VPN connection. A CRL Distribution Point (CDP) resides on a different network than the CA that produced the CRL it hosts. An Outer CDP resides on a Black network, and hosts a CRL created by the CA on a Gray network. Similarly, an Inner CDP resides on a Gray network, and hosts a CRL created by the CA on a Red network. Because the CDP and its CA reside on different networks, a one-way transfer mechanism is needed to periodically distribute the current CRL from the CA to the CDP; the details of the one-way transfer mechanism are left to a solution's Authorizing Official (AO).

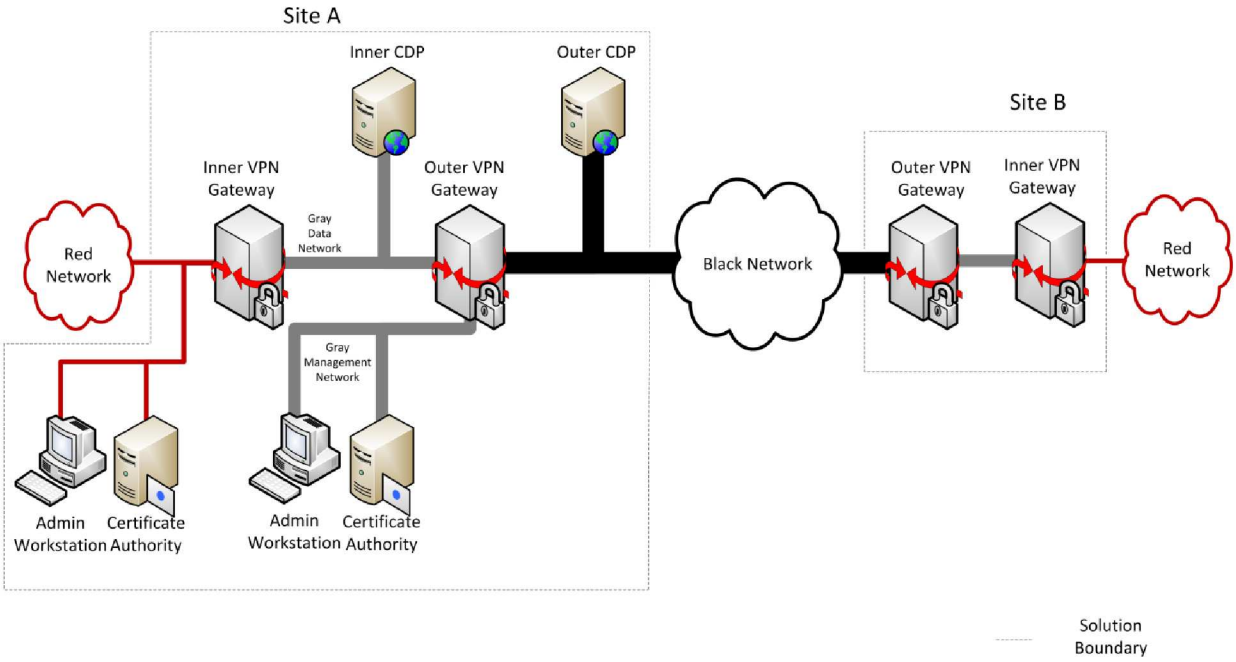


**Figure 7. VPN Solution using CRL Distribution Points**

Figure 7 illustrates the placement of CDPs to make CRLs accessible to Remote Sites on the Black network before VPN tunnel establishment. During negotiation of the outer VPN tunnel, the Outer VPN Gateways contact the Outer CDP on the Black network to download the latest CRL produced by the Gray CA. Similarly, during negotiation of the inner VPN tunnel, the Inner VPN Gateways contact the Inner CDP on the Gray network to download the latest CRL produced by the Red CA.

The use of CDPs on the external side of the VPN Gateways requires that the contents of the CRLs hosted on them are unclassified, since the CDPs are located on networks that the design of the VPN solution treats as unclassified. If a solution owner's classification authority decides that its CRLs are classified, then its VPN solutions would be unable to make use of external CDPs.

For solutions that support networks of different security levels (see Section 4.3.2), a single Inner CDP may be used to host the CRLs for the Inner VPN Gateways of multiple Red networks.

A solution owner may choose to implement zero, one, or multiple CDPs on Black and Gray networks, based on their expected utility in facilitating CRL distribution to Remote Sites. Having multiple redundant CDPs on the same network improves the availability of CRL distribution, since a VPN Gateway only needs to be able to contact one CDP in order to obtain the CRL. Conversely, in a small-scale solution, manual out-of-band distribution of CRLs may be more cost-effective than deploying and maintaining CDPs.

## 4.4 RATIONALE FOR LAYERED ENCRYPTION

A single layer of Suite B encryption, properly implemented, is sufficient to protect classified data in transit across an untrusted network. The VPN solution uses two layers of Suite B encryption not because of a deficiency in the cryptographic algorithms themselves, but rather to mitigate the risk that a failure in one of the VPN Gateways, whether by accidental misconfiguration, operator error, or malicious exploitation of an implementation vulnerability, which could result in exposure of classified information. The use of multiple layers of protection reduces the likelihood that any specific vulnerability can be exploited to attack the full solution, particularly if the layers exhibit suitable independence.

If an Outer VPN Gateway is compromised or fails in some way, the Inner VPN Gateway can still provide sufficient encryption to prevent the immediate exposure of classified data to a Black network. In addition, the Inner VPN Gateway can indicate that a failure of the Outer VPN Gateway has occurred, since the filtering rules applied to its Gray network interface will drop and log the receipt of any non-IPsec packets. Such log messages indicate that the Outer VPN Gateway has been breached or misconfigured to permit traffic to pass through to the Inner VPN Gateway that is not allowed.

Conversely, if instead the Inner VPN Gateway is compromised or fails in some way, the Outer VPN Gateway can likewise still provide sufficient encryption to prevent the immediate exposure of classified data to a Black network. As in the previous case, the filtering rules applied to its Gray network interfaces will drop and log the receipt of any non-IPsec packets from the Inner VPN Gateway. Such log messages indicate that the Inner VPN Gateway has been breached or misconfigured to permit traffic to pass through to the Outer VPN Gateway that is not allowed.

If both the Outer and Inner VPN Gateways are both compromised or fail simultaneously, then it may be possible for classified data from the Red network to be sent to a Black network without an adequate level of encryption. The security of the VPN solution depends on preventing this failure mode by promptly remediating any compromises or failures in one VPN Gateway before the other VPN Gateway also fails or is compromised.

Diversity of implementation is needed between the components in each layer of the solution in order to reduce the likelihood that both layers share a common vulnerability. The CSfC Program recognizes two ways to achieve this diversity. The first is to implement each layer using components produced by different manufacturers. The second is to use components from the same manufacturer, where that manufacturer has provided NSA with sufficient evidence that the implementations of the two components are independent of one another. The CSfC web page (http://www.nsa.gov/ia/programs/csfc_program) contains details for how a manufacturer can submit this evidence to NSA and what documentation must be provided. Customers wishing to implement a solution in accordance with this Capability Package that uses products from the same manufacturer in both layers should contact their NSA/IAD Client Advocate to confirm that NSA has accepted the manufacturer's claims before implementing their solution.

## 4.5 AUTHENTICATION

The VPN solution provides mutual device authentication between VPN Gateways during tunnel setup via public key certificates, but does not provide any end user authentication for traffic going through the tunnels. In general, any end user authentication between two sites required by the customer must be provided separately and will not be considered as a part of this solution.

## 4.6 OTHER PROTOCOLS

Throughout this document, when IP traffic is discussed, it can refer to either IPv4 or IPv6 traffic, unless otherwise specified. In addition, Red, Gray and Black networks can run either version, and each network is independent from the others in making that decision. In the remainder of the document, if no protocols or standards are specified then any appropriate protocols may be used to achieve the objective.

Public standards conformant Layer 2 control protocols such as Address Resolution Protocol (ARP) are allowed as necessary to ensure the operational usability of the network. This Capability Package is agnostic with respect to Layer 2; specifically, it does not require Ethernet. Public standards conformant Layer 3 control protocols such as Internet Control Message Protocol (ICMP) may be allowed based on local AO/Designated Approving Authority (DAA) policy, but the default configuration of this solution is for all Layer 3 control protocols to be disabled. Red and Gray network multicast messages and Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) may also be allowed depending on local AO/DAA policy. Multicast messages received on external interfaces of the Outer VPN Gateway shall be dropped.

It is expected that the VPN solution can be implemented in such a way as to take advantage of standards based routing protocols that are already being used in the network. For example, networks that currently use Generic Routing Encapsulation (GRE) or Open Shortest Path First (OSPF) protocols can continue to use these in conjunction with this solution to provide routing as long as the AO/DAA approves their use.

## 4.7 AVAILABILITY

The high-level designs described in Section 4.3 are not designed with the intent of automatically providing high availability, and supporting solution implementations for which high availability is important is not a goal. However, this Capability Package does not prohibit adding redundant components in parallel to allow for component failover or to increase the throughput of the VPN solution, as long as each redundant component adheres to the requirements of this Capability Package.

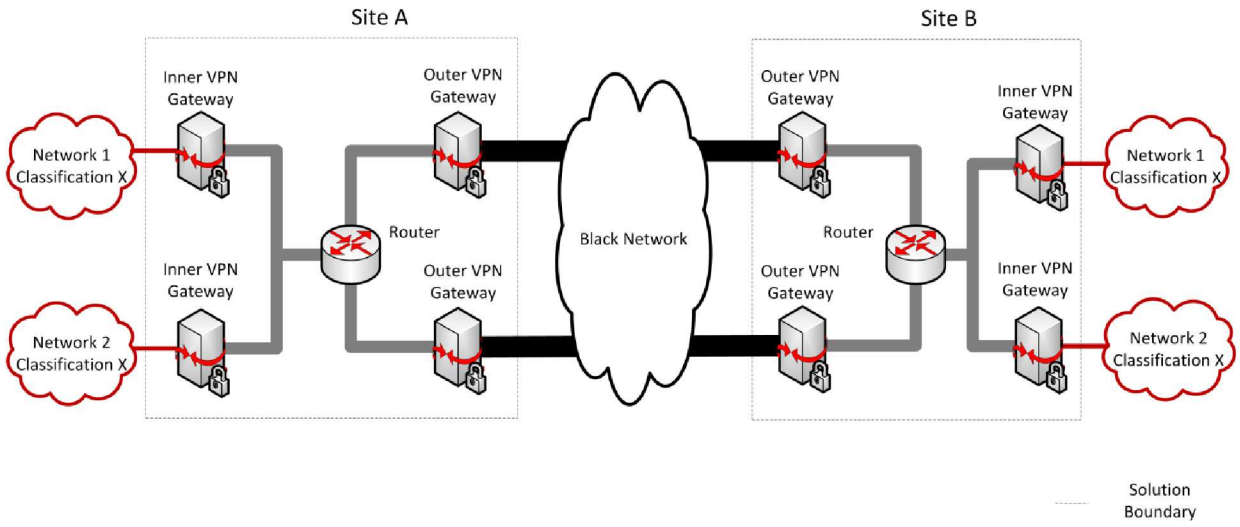


**Figure 8. VPN Solution with Redundant Outer VPN Gateways**

For example, Figure 8 illustrates a VPN solution between two sites where each site has a redundant Outer VPN Gateway. (Management components are omitted from the figure for clarity.) There are two outer VPN tunnels that transit the Black network: one between the upper pair of Outer VPN Gateways, and one between the lower pair of Outer VPN Gateways. Each site's Gray network contains an ordinary router between the Inner and Outer VPN Gateways which selects which Outer VPN Gateway to route outbound packets to. This router is part of the solution only in the sense that it is part of the network infrastructure of the Gray network; this Capability Package does not levy any security requirements on the router. The VPN solution can maintain connectivity between the two sites even if one of the Outer VPN Gateways fails, because traffic will be routed through the tunnel that has not failed.

The above is only a simple example of how redundancy could be added if needed for a VPN solution. Implementing standby or failover VPN Gateways, performing load balancing between VPN Gateways, or other techniques to improve the availability or throughput of the solution are outside the scope of this Capability Package and are not discussed further.

# 5 SOLUTION COMPONENTS

In the high-level designs discussed in the previous section, all communications flowing across a Black network are protected by at least two layers of encryption, implemented using IPsec VPN tunnels generated by VPN Gateways within the network infrastructure. Additionally, mandatory aspects of the solution include Administration Workstations and CAs for key management using Public Key Infrastructure (PKI).

Each component is described in more detail below. The descriptions include information about the security provided by the components as evidence for why they are deemed mandatory for the solution.

Overall System Security is discussed in Section 7. Approved components can be found on CSfC Component List.

Additional components are discussed in Section 5.7 can be added to the solution to help reduce the overall risk. However, these are not considered mandatory components for the security of the solution; therefore, this Capability Package does not place configuration or security requirements on the components.

## 5.1 Outer VPN Gateways

Authentication of peer VPN Gateways, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules are all aspects fundamental to the security provided by VPN Gateways.

The Outer VPN Gateway is located at the edge of the private network and generates an IPsec tunnel, which provides device authentication and confidentiality and integrity of information traversing Black networks. VPNs offer a decreased risk of exposure of information in transit since any information that traverses a Black network is placed in a secure tunnel that provides an authenticated and encrypted path between two sites.

Although the Outer VPN Gateway is a perimeter VPN Gateway and thus more exposed to external attacks, the VPN Gateway is also capable of protecting the network from unauthenticated traffic through use of an internal filtering capability. This allows specification of rules that prohibit unauthorized data flows, which helps mitigate Denial of Service (DoS) attacks and resource exhaustion. This solution does not require that the Outer VPN Gateway terminate all VPNs on a single physical interface; however, all such external interfaces shall conform to the port filtering requirements in Section 10.5. The Outer VPN Gateway is implemented identically for all the high-level designs covered in this Capability Package.

Outer VPN Gateways are also responsible for filtering traffic on its Gray network interfaces to prevent Inner VPN Gateways for networks of different classification levels from being able to send packets to one another. Since this filtering is primarily based on the source and destination addresses in the packet on a Gray network, the Gray networks themselves must use an addressing scheme that supports the necessary filtering (such as using separate address ranges for the Gray interfaces of Inner VPN Gateways supporting each Red network). This filtering on Gray network traffic is performed even for solutions that only support Red networks of a single classification level, as in that situation the actual filtering needed to comply with this Capability Package would be simple.

In addition to performing the functions described in this Capability Package, an Outer VPN Gateway may also use AO/DAA-approved routing protocols on the Gray network it is connected to. The Outer VPN Gateway cannot route packets between Gray and Black networks; any packets received on a Gray

network interface and sent out a Black network interface must be transmitted within an IPsec VPN tunnel configured according to this Capability Package. There is some data that will originate from the Outer VPN Gateway (such as control traffic (e.g. Bidirectional Forwarding Detection (BFD)), logging and audit data, which will potentially be sent to a Gray Management network at another site) that will only go through the outer IPsec tunnel. This is the only exception to having two layers of encryption for data going over a Black network and is considered acceptable given the limited intelligence value of that information and the fact that it does not contain classified data. However, management traffic on a Gray network, which originates from the Administration Workstation, must include two layers of encryption as described in this Capability Package (see Section 10.7).

## 5.2 Inner VPN Gateways

Similar to the Outer VPN Gateway, the Inner VPN Gateway provides authentication of peer VPN Gateways, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules.

In addition to performing the functions described in this Capability Package, an Inner VPN Gateway may also use AO/DAA-approved routing protocols on the Red network it is connected to. The Inner VPN Gateway shall not route packets between Red and Gray networks; any packets received on a Red network interface and sent to a Gray network interface must be transmitted within an IPsec VPN tunnel configured according to this Capability Package.

## 5.3 Certificate Authorities

The CA's are responsible for issuing digital certificates for the VPN Gateways in this solution. These certificates are used for authentication in establishing the IPsec tunnels between pairs of VPN Gateways. Given the high-level design of the solution, there are distinct CAs for the Inner and Outer VPNs. The CA providing certificates for Inner VPN Gateways is located on a Red network, and the CA providing certificates for Outer VPN Gateways is located on a Gray Management network. This provides additional key management separation between the two independent layers of encryption.

If the solution is supporting Red networks of different security levels, then a separate CA is needed for the Inner VPN Gateways of each security level.

If the organization has existing enterprise CAs that satisfy the requirements of this Capability Package, those CAs should be used as part of the VPN solution rather than setting up new CAs dedicated to this solution.

## 5.4 Administration Workstations

Each component in the solution has one or more Administration Workstations that are responsible for maintaining, monitoring, and controlling all security functionality for that component. Throughout this

document, these Workstations are referred to as the Administration Workstation. It should be understood that all of the required administrative functionality does not need to be present in each individual Workstation, but the entire set of Administration Workstations must collectively meet administrative functionality requirements.

The Administration Workstation is used for logging and configuration review and management. Implementations may employ a separate Audit Workstation for log management, but the Administration Workstation will be able to perform log review. Given the architecture of the solution, each layer has its own distinct administration LAN or VLAN: the Inner VPN Gateway and supporting components are managed from a Red network, and the Outer VPN Gateway and supporting components are managed from a Gray network. This architecture provides the separation necessary for two independent layers of protection.

Administration Workstations will be dedicated for the purposes given in the Capability Package. For example, Administration Workstations are not to be used as the registration authority for the CA, a log server, or as a general user workstation for performing any functions besides management of the solution. Administration Workstations cannot be used as an enrollment workstation or provisioning workstation. Administration Workstations may be used to manage multiple CSfC solutions on the same Red or Gray network.

For VPN solutions with multiple Red networks with different security levels using a single Outer VPN Gateway a separate Administration Workstation is needed to manage the Inner VPN Gateways of each security level.

The VPN solution described in this Capability Package includes a log server on each Gray and Red network that receives logs forwarded from devices on those networks. Given a Cross Domain Solution (CDS) approved by the AO/DAA to transfer data from an unclassified network to a network classified at the level of a Red network, that CDS could be used to copy log data from a Gray network log server to a Red network log server. Having Gray network logs on the Red network could simplify monitoring of the solution, since having a separate log monitoring capability on the Gray network would no longer be necessary. The requirements for a CDS capable of securely transferring log data from an unclassified network to a classified network are outside the scope of this Capability Package.

## 5.5 Gray Network Firewalls

A VPN solution that supports multiple Red networks may include one or more Gray Network Firewalls, as described in Section 4.3.2.2. The primary purpose of a Gray Network Firewall is to block any packets sent between Inner VPN Gateways for Red networks of different classification levels. A Gray Network Firewall also blocks any packets sent between management components on the Gray network and Inner

VPN Gateways for Red networks that operate at a classification level other than the highest classification level of data protected by the solution.

A standalone Gray Network Firewall would typically only be used in solutions where the physical design of the Gray network includes paths between Inner VPN Gateways for Red networks of different classification levels that do not pass through the Outer VPN Gateway. Effectively, each Gray Network Firewall is another instance of the Gray network filtering performed by the Outer VPN Gateway. See Section 5.1 for more information about the filtering performed on Gray network traffic.

## 5.6 Certificate Revocation List (CRL) Distribution Points (CDP)

A Certificate Revocation List (CRL) Distribution Point (CDP) is a server other than a CA that makes CRLs available to VPN Gateways within a solution. As described in Section 4.3.3, a VPN solution may use CDPs to provide CRLs to VPN Gateways before those VPN Gateways have established any VPN tunnels. For this to work, the CDPs are placed on the network reachable from the VPN Gateway's external interface: on the Black network for Outer VPN Gateways and on the Gray network for Inner VPN Gateways.

A CDP is a web server whose sole function is to host copies of one or more CRLs for VPN Gateways to download before performing mutual authentication with one another during tunnel establishment. CDPs do not serve any other content, and in particular do not host any dynamically-generated content, nor do they provide any other services. Minimizing the attack surface is particularly important for an Outer CDP; since it is connected to the Black network, it is more exposed to external attack than most other components in the solution.

A CDP is located on a different network than the CA that issues the CRLs it hosts: an Outer CDP is on the Black network but hosts CRLs issued by a Gray CA, and an Inner CDP is on the Gray network but hosts CRLs issued by a Red CA. In order to copy new CRLs from a CA to a CDP, a one-way transfer mechanism is necessary. The transfer mechanism must be one-way, to prevent a return path from allowing malicious content to bypass a VPN Gateway and enter a Gray or Red network. The AO for the solution is given discretion to select a one-way transfer mechanism to use, which could be process-based (such as copying via write-once removable media) or technology-based (such as an approved cross-domain solution). To use CDPs, it is also necessary to treat the CRLs themselves as unclassified, since the CDPs are located on the Black network for Outer VPN Gateways and on the Gray network for Inner VPN Gateways.

CDPs serve CRLs over unencrypted Hypertext Transfer Protocol (HTTP) connections instead of TLS-encrypted Hypertext Transfer Protocol Secure (HTTPS) connections, because HTTPS would provide little additional security benefit. A CRL contains the minimal set of information necessary to be used by the VPN Gateways, so there are few concerns with the confidentiality of the CRL's contents. A CRL's integrity is protected by the digital signature of the CA that issued it, so additional integrity protection in transit is unnecessary. Providing the CRLs over HTTPS would introduce a potential circular dependency: a VPN Gateway would need the CRL to determine whether the CDP's TLS certificate was revoked, but could not

obtain the CRL until the CDP successfully authenticates itself to the VPN Gateway. Serving CRLs over ordinary HTTP follows the recommendation in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 5280 not to use HTTPS to distribute CRLs.

There may be multiple Inner CDPs or Outer CDPs within a solution. Additional CDPs provide redundancy should a CDP fail or become unavailable, since a VPN Gateway would only need to contact one of the CDPs in order to obtain the latest CRL.

CDPs may host delta CRLs in addition to complete CRLs. In large VPN solutions, the use of delta CRLs can reduce the amount of network traffic needed to distribute updated CRLs to each participating site.

This Capability Package does not require that CDPs be used within a solution, although it does levy requirements on any CDPs that are implemented. CDPs are expected to be used in large VPN solutions where manual, out-of-band CRL distribution is costly, difficult, or infeasible to achieve in a timely manner. CDPs allow CRLs to be distributed to large numbers of VPN Gateways in a mostly automated fashion.

## 5.7 Other Controls

There are additional controls that could be used within this solution to potentially reduce the overall risk.

First, a screening router can be used to filter packets from Black networks before they arrive at Outer VPN Gateways and Outer CDPs. The screening router could be part of an existing Black network (e.g. Customer Edge Router), or could be added between Outer VPN Gateways and existing Black network components. However, since the screening router would become part of a Black network, it is not considered to be part of the VPN solution itself.

Second, a more comprehensive Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) could be used if additional assurance is desired. In particular, a comprehensive IDS or IPS system on a Gray network could increase the difficulty of a rogue actor evading detection, since normal, legitimate traffic on a Gray network is relatively easy to characterize. However, an IDS or IPS on a Gray network would need to be standalone, as it would not be able to interconnect with similar systems on a Red or Black network. Although an IDS or IPS is not required, if they are chosen to be implemented relevant Objective requirements are included in Section 10.8.

Additionally, Auditors could monitor user connection metrics for anomalies and monitor individual user sessions. All monitoring of user sessions and metrics would be conducted from a Red network.

Finally, if an integrator is used for implementation of this solution, the customer can require separation of roles between individuals working on Red and Gray components. The separation of roles ensures that

during the development of the solution no single individual can compromise Red and Gray components simultaneously.

# 6 KEY MANAGEMENT

One of the most difficult parts of any solution is determining how the key management will be implemented in a secure manner. In this solution, the only certificates necessary are for the device authentication certificates on each of the two VPN Gateways at the end of each IPsec tunnel. The certificates and private keys used in the solution are considered Controlled Unclassified Information (CUI), because they are only used for mutual device authentication, not for traffic encryption.

No single CA can provide keys to both Inner and Outer VPN Gateways. The CAs for Outer VPN Gateways are located on a Gray Management network, connected to an Outer VPN Gateway. A Locally-run CA may need to be stood up to key Outer VPN Gateways, requiring that a CA product be selected from the NSA-approved CSfC Component List for Outer tunnel PKI. In addition, a Certificate Policy (CP)/Certification Practice Statement (CPS) document must be created or tailored for each CA used in the solution. It is then the AO/DAA's responsibility to approve the use of a CA. If an Outer tunnel CA is an Enterprise CA already running on the necessary Gray Management network, no additional approval is necessary for use of the CA.

CAs for Inner VPN Gateways are located on Red networks, which may allow for use of existing Enterprise CAs already operational on the Red network, following the requirements in Section 10.9.2 of this Capability Package. For networks in which an existing Enterprise CA is not available, the use of a Locally-run CA on the Red network, following the requirements in Section 10.9.3, is an acceptable alternative. If an Inner tunnel CA is an Enterprise CA already running on a Red network, no additional approval is necessary for use of this CA. For example, a solution may use an Enterprise CA (such as a Committee on National Security Systems (CNSS)-approved CA, which follows Committee on National Security Systems Instruction (CNSSI) 1300 under the National Security Systems (NSS) PKI Root CA, to issue certificates to an Inner VPN Gateway. If, however, an Inner tunnel CA uses a Locally-run CA on a Red network, the approval process given in the preceding paragraph for an Outer tunnel CA applies and must be followed.

Each VPN Gateway has at least one CA signing certificate (sometimes referred to as a Trust Anchor), which is used by the VPN Gateway to authenticate to other VPN Gateways in the solution. If centralized management is used throughout the solution, there will be only one CA signing certificate in each VPN Gateway. Otherwise, one CA signing certificate is installed in each Inner VPN Gateway for each Inner Tunnel CA used in the system. Similarly, one CA signing certificate will be installed in each Outer VPN Gateway for each Outer Tunnel CA used in the system.

Each VPN Gateway will contain a private key that corresponds to a certificate issued by its CA, and one or more CA signing certificates as described above. Each VPN Gateway will also contain revocation information. The private key may be locally generated and must be adequately protected. Both Inner

and Outer tunnel PKIs shall use Elliptic Curve Digital Signature Algorithm (ECDSA) over the curve P-384 with SHA-384 or RSA 3072 bit or greater signatures within X.509 certificates. The algorithms and elliptic curves that are approved for use in this VPN solution are found in Table 6 (see Section 10.2).

The VPN solution described here requires certificates to establish the secure tunnels between VPN Gateways. Without certificates, the network cannot function. Thus, an out-of-band method must be used to issue the initial certificates to the VPN Gateways. Subsequent rekeying, however, should take place over the network through this solution prior to the current key's expiration. The key validity period for certificates issued by Locally-run CAs cannot exceed 14 months, while the key validity period for certificates issued by an Enterprise CA are inherited from the Enterprise CA certificate policy. Updates to CRLs are distributed to VPN Gateways within 24 hours of CRL issuance.

# 7 THREATS

This section details how the required components work together to provide overall security in the solution. (Figure 2 through Figure 8) show the boundary of the VPN solution for each high-level design covered by this Capability Package.

An assessment of security was conducted on each of the high-level designs described in this Capability Package while making no assumptions regarding use of specific products for any of the defined components. There are several different threats to consider when evaluating the risk of transporting data over secure or unsecure networks. By examining these threats, the organization can have a better understanding of the risks they are accepting by implementing the solution and how these risks affect the Confidentiality, Integrity, and Availability of the network, systems, and data.

## 7.1 PASSIVE THREATS

This threat refers to internal or external actors attempting to gain information from the network without changing the state of the system. Threat actions include collecting or monitoring traffic (e.g. traffic analysis or sniffing the network) passing through a network in order to gain useful information through data analysis.

The security against a passive attack targeting the data in transit across the Black network is provided by the layered IPsec tunnels. To mitigate passive attacks, two layers of Suite B encryption, Advanced Encryption Standard (AES), are employed to provide confidentiality for the solution. Use of AES is approved to protect classified information, meeting IAD and CNSSP-15 guidance for adequate confidentiality. The Inner and Outer VPN Gateways that are used to set up the two tunnels must be independent in a number of ways (see Section 9). Due to this independence, the adversary should not be able to exploit a single cryptographic implementation to compromise both tunnels.

The use of one or more Outer CDPs to distribute unencrypted CRLs on a Black network potentially allows a passive threat actor with access to the Black network path between an Outer CDP and Outer VPN Gateway to obtain a copy of the CRL issued by a Gray CA. However, the content of the CRL is primarily limited to a list of serial numbers of revoked certificates, the date and time when each certificate was revoked, and a high-level reason why each certificate was revoked (such as key compromise or cessation of operation). The CRL does not specify what certificates are still valid, nor does it identify the physical or network locations of any components in the solution. The CRL also does not reveal any information about certificates issued by anything other than the Gray CA. If a solution owner's AO/DAA considers the limited information in a CRL too sensitive to distribute on the Black network, the solution owner can choose not to implement Outer CDPs and rely on other means to distribute CRLs to Outer VPN Gateways in a timely fashion.

## 7.2 External (Active) Threats

This threat refers to outsiders gaining unauthorized access to a system or network, exfiltration of sensitive Red network data, or degradation of availability of the system or network. Threat actions include introducing viruses, malware, or worms with the intention to compromise the network or exfiltrate data, or to analyze the design of the network or system for future attacks. Adversaries could gain access to a VPN Gateway, and then exploit or compromise other devices on the network. DoS or Distributed DoS (DDoS) attacks compromise availability of the system, degrading/disrupting secure communication across a Black network. Further external threat actions would include social engineering attacks to assist attackers with gaining additional access to a network for the purpose of compromising a system or network, traffic injection or modification attacks, or replay attacks.

### 7.2.1 Rogue Traffic

One method for detecting rogue traffic from an external attack as it attempts to pass through one or both VPN Gateways is by having the port filtering native to each VPN Gateway enabled and configured to audit and log any traffic that is not of the format described in the configuration (see Section 10.5). It is required that the port filtering be set up to block: 1) any traffic not coming from or going to an IP address on the network at the other site, 2) traffic not contained in IP packets other than control plane protocols needed for network operation and approved by AO/DAA policy, and 3) traffic going to unexpected ports. This will allow the Auditor(s) and/or the Security Administrator(s) (see Section 12) to detect whether the Outer VPN Gateway has been breached, thus providing an early warning of a potential intrusion. It will also provide detection of misconfigured Outer VPN Gateways.

Another method for detecting a potential intrusion into the solution is requiring automated configuration change detection on Red and Gray Management networks to ensure VPN Gateway configurations are not changed without the knowledge of Auditors and Security Administrators. Auditors also ensure through the audit logs that all configuration changes are valid. This will counter attacks that take advantage of VPN Gateway misconfigurations.

CDPs are protected from rogue traffic by implementing port filtering on the server. Rogue traffic to CDPs can be further mitigated by implementing a firewall or other packet filtering device between the CDP and the rest of the network.

### 7.2.2 Malware and Untrusted Updates

The Administration Workstations and CAs for a Red network shall be distinct from the Administration Workstations and CAs for a Gray network. This separation will minimize the potential for malware on a single device to impact components supporting both Inner and Outer VPN tunnels.

Each individual component of this solution has the capability to perform trusted updates through verification of a signature or hash to ensure that the update is from a reliable source, such as signed by the vendor. This mitigates threats of malicious users trying to push updates or code patches that affect the security of the component (and therefore system). The source of all updates and patches should be verified before installation occurs.

### 7.2.3 Denial of Service

DoS attack risks cannot be completely mitigated. VPN solutions in compliance with this Capability Package are required to drop all packets that are not Internet Key Exchange (IKE), Encapsulating Security Payload (ESP), or other approved protocols on the appropriate interfaces, which significantly reduces the potential of flooding attacks. For customers that require more protection against these attacks, one option is the use of a perimeter router between the Outer VPN Gateway and Black networks to filter traffic before it reaches the Outer VPN Gateway. Another option for customers requiring more protection is to add additional filtering based on specifics like known network IP addresses to filter traffic from devices not included in this solution or leasing private lines for the Black network. Other mitigations are acceptable and up to the AO/DAA to approve their use.

A single VPN Gateway failure is likely to result in a DoS condition. One assumption underlying this solution is that high assurance of availability is not required. If availability is critical for the customer both network redundancy and instituting DoS response procedures when loss of availability is detected can provide further protection against DoS attacks.

When using Outer CDPs to distribute CRLs to Outer VPN Gateways on a Black network, a sustained DoS attack on the CDPs could prevent Outer VPN Gateways from receiving updated CRLs. If the CRLs cached at the other VPN Gateways then expire, they would be unable to establish VPN connections due to the inability to check the revocation status of certificates during the mutual authentication process. Deploying multiple Outer CDPs reduces the likelihood of a successful DoS attack on this part of the solution, since as long as even one Outer CDP is available, Outer VPN Gateways will be able to retrieve CRL updates. Additionally, a solution using CDPs should still have procedures in place for out-of-band CRL distribution to use in the event that all Outer CDPs become unavailable.

### 7.2.4 Social Engineering

It is the responsibility of the customer to define the appropriate policies and training necessary to protect against Social Engineering attacks. In addition, these types of attacks generally take advantage of other attacks detailed in this section and already discussed.

## 7.3 Insider Threats

This threat refers to an authorized or cleared person or group of people with physical or logical access to the network or system who may act maliciously or negligently, resulting in risk exposure for the organization. This threat could include poorly trained employees, curious employees, disgruntled employees, escorted personnel who gain access to the equipment, dishonest employees, or those that have the means and desire to gain escalated privileges on the network.

Threat actions include insertion or omission of data entries that result in a loss of data integrity, unintentional access to an unauthorized system or network, willingly changing the configuration of an , unwillingly or unknowingly executing a virus or malware, intentionally exposing the network and systems to viruses or malware, cross-contaminating a system or network with data from a higher classification to a lower classification (e.g. Secret data to an Unclassified network or system), or malicious or unintentional exfiltration of classified data. Typically, the threat from insiders has the potential to cause the greatest harm to an organization, and insider attacks are also the hardest to monitor and track.

To mitigate insider threats, separation of roles within the solution is required (see Section 12). In addition, logging and auditing of security critical functionality (see Section 10.8) is required. Also, strong authentication of the Security Administrator and Auditor are required for access to ensure accountability of these individuals. Finally, outbound filters on VPN Gateways and s are configured to look for traffic leaving the internal network that does not go through the IPsec tunnels. In scenarios that need additional assurance, an IDS could be deployed on the Gray network between an Outer VPN Gateway and other solution components to help identify unusual or suspicious traffic that could result from a failure, misconfiguration, or attack on Inner or Outer VPN Gateways.

## 7.4 Supply Chain Threats

A critical aspect of the U.S. Government's effectiveness is the dependability, trustworthiness, and availability of the Information and Communication Technology (ICT) components embedded in the systems and networks upon which the ability to perform U.S. Government missions rely. The supply chain for those ICT components are the underpinnings of those systems and networks and supply chain attacks are attempts to proactively compromise those underpinnings.

Unfortunately, the supplier cannot always provide guarantees of a safe delivery of a component; they are only able to provide assurances based on their reliance of established procedures and processes

they have developed. In a single change of hands, the component may be introduced to potential threats and compromises on many levels.

The supply chain threat refers to an adversary gaining access to a vendor or retailer and then attempting to insert or install a modification or a counterfeit piece of hardware into a component that is destined for a U.S. Government customer in an effort to gain information or cause operational issues. This threat also includes the installation of malicious software on components of the solution. This threat is difficult to identify and test, and is increasingly more difficult to prevent or protect against since vendors build products containing components manufactured by subcontractors. It is often difficult to determine where different pieces of components are built and installed within the supply chain.

Threat actions include manufacturing faulty or counterfeit parts of components that can be used to disrupt system or network performance, leaving open back doors in hardware that allow attackers easy ways to attack and evade monitoring, as well as easy ways to steal data or tamper with the integrity of existing/new data. Supply Chain attacks may occur during development and production, updates, distribution, shipping, at a warehouse, in storage, during operations, or disposal. For this reason, it is imperative that all components selected for use in CSfC solutions are subject to the applicable Supply Chain Risk Management (SCRM) process to reduce the risk of acquiring compromised components.

Each component that is selected from the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO/DAA-approved Product Supply Chain Threat Assessment process (See CNSSD 505 Supply Chain Risk Management (SCRM) for additional guidance).

There are doctrinal requirements placed on Product Selection, Implementers, and System Integrators of these solutions to minimize the threat of supply chain attacks (see Sections 9, 11, and 12).

## 7.5 Integrator Threats

This threat refers to an integrator who has unrestricted access to all components within the solution prior to the customer purchasing and implementing the solution within their system. This is different than a Supply Chain threat in that these integrators have access to all components to be used in the solution, rather than only those being procured from a particular vendor.

Threat actions could include installing or configuring components in a manner that places the organization at risk for attack or open to an unknown vulnerability that may not be detected through normal tests, scans, and security counter-measures.

In order to mitigate this threat, integrators are required to be cleared to the highest level of data protected by the VPN solution. To further reduce the integrator threat, a customer may wish to use multiple integrators, such that no one integrator has access to all components of the solution.

# 8 REQUIREMENTS OVERVIEW

The following five sections (Sections 9 through 13) specify requirements for implementations of VPN solutions compliant with this Capability Package. However, not all requirements in the following sections will apply to each compliant solution. Sections 8.1 and 8.2 describe how to determine which set of requirements applies to a particular solution.

## 8.1 CAPABILITIES

This Capability Package provides the flexibility needed to implement a variety of designs that use VPNs to provide different capabilities. Although most requirements are applicable to all solutions, some requirements are only applicable to implementations whose high-level designs implement certain features.

**Table 1. Capability Designators**

| Capability | Designator | Description |
|---|---|---|
| Multiple Sites | M | VPN solutions that interconnect two or more sites, as described in Sections 4.3.1 and 4.3.2. |
| Gray Network Firewalls | F | VPN solutions that include Gray Network Firewalls, as described in Sections 4.3.2.2 and 5.5. This capability cannot be implemented without also implementing capability M, R, and/or L. |
| CDPs | C | VPN solutions that include CDPs, as described in Sections 4.3.3 and 5.6. This capability cannot be implemented without also implementing capability M, R, and/or L. |

Any solution that follows this Capability Package must implement at least one of the above capabilities, and may implement multiple capabilities. The “Capabilities” column in the requirements tables in Sections 9 through 13 identifies which capabilities the requirement applies to. A requirement is only applicable to a solution if the “Capabilities” column for that requirement lists one or more of the capabilities being implemented by the solution.

A small number of requirements apply only to solutions that implement *both* the Gray Network Firewalls (F) *and* the CDPs (C) capabilities. These requirements have “F+C” listed in the “Capabilities” column.

For example, suppose that a VPN solution is designed to interconnect enclaves of a classified network across a large number of sites, and uses CDPs to facilitate distribution of CRLs. This solution implements the Multiple Sites (M) and CDPs (C) capabilities. Any requirement that lists “M” or “C” in the Capabilities column is applicable to the solution. Requirements that only list “F” or “F+C” are not applicable, and do not need to be implemented (and may not be possible to implement) by the solution in order to comply with this Capability Package.

## 8.2 THRESHOLD AND OBJECTIVE REQUIREMENTS

In some cases, multiple versions of a requirement may exist in this Capability Package. Such alternative versions of a requirement are designated as being either a Threshold requirement or an Objective requirement:

- A Threshold (T) requirement specifies a feature or function that provides the minimal acceptable capability for the security of the solution.
- An Objective (O) requirement specifies a feature or function that provides the preferred capability for the security of the solution.

In general, when separate Threshold and Objective versions of a requirement exist, the Objective requirement provides a higher degree of security for the solution than the corresponding Threshold requirement. However, in these cases meeting the Objective requirement may not be feasible in some environments or may require components to implement features that are not yet widely available. Solution owners are encouraged to implement the Objective version of a requirement, but in cases where this is not feasible solution owners may implement the Threshold version of the requirement instead.

The "Threshold / Objective" column in the requirements tables in Sections 9 through 13 identifies whether a particular requirement is Threshold (T) or Objective (O). When a distinction between Threshold and Objective exists, the "Alternative" column lists which other requirement or requirements may be implemented instead in order to comply with this Capability Package. For example, if a solution does not implement Objective requirement VPN-CR-12, it can implement the corresponding Threshold requirement VPN-CR-11 instead. Conversely, if a solution does implement Objective requirement VPN-CR-12, then it would not also implement VPN-CR-11; when separate Threshold and Objective requirements exist, they are mutually exclusive.

In most cases there is no distinction between the Threshold and Objective versions of a requirement. In these cases, the "Threshold / Objective" column indicates that the Threshold equals the Objective (T=O), and the "Alternative" column is blank. Such requirements must be implemented in order to comply with this Capability Package, as long as the requirement is applicable per Section 8.1.

Requirements that are listed as Objective in this Capability Package may become Threshold requirements in a future version of this Capability Package. Solution owners are encouraged to implement Objective requirements where possible in order to facilitate compliance with future versions of this Capability Package.

## 8.3 REQUIREMENTS DESIGNATORS

Each requirement defined in this Capability Package has a unique identifier consisting of the prefix "VPN," a digraph that groups related requirements together (e.g. KM), and a sequence number (11).

Table 3 lists the digraphs used to group together related requirements and identifies the sections in which those requirement groups can be found.

**Table 2. Requirement Digraphs**

| Digraph | Description | Section | Table |
|---|---|---|---|
| PS | Product Selection Requirements | Section 9 | Table 3 |
| SR | Overall Solution Requirements | Section 10.1 | Table 4 |
| CR | Configuration Requirements for All VPN Gateways | Section 10.2 | Table 6 |
| IR | Additional Requirements for Inner VPN Gateways | Section 10.3 | Table 7 |
| OR | Additional Requirements for Outer VPN Gateways | Section 10.4 | Table 8 |
| PF | Port Filtering Requirements for VPN Gateways | Section 10.5 | Table 9 |
| CM | Configuration Change Detection Requirements | Section 10.6 | Table 10 |
| DM | Requirements for Device Management | Section 10.7 | Table 11 |
| AU | Auditing Requirements | Section 10.8 | Table 12 |
| KM | Key Management Requirements | Section 10.9 | Table 13<br>Table 14<br>Table 15 |
| FW | Gray Network Firewall Requirements | Section 10.10 | Table 16 |
| CD | Requirements for CDP Devices | Section 10.11 | Table 17 |
| GD | Requirements for the Use and Handling of Solutions | Section 11.1 | Table 18 |
| | Role-Based Personnel Requirements | Section 12 | Table 20 |
| RP | Incident Reporting Requirements | Section 11.2 | Table 19 |
| TR | Test Requirements | Section 13 | Table 21 |

# 9 REQUIREMENTS FOR SELECTING COMPONENTS

In this section, a series of requirements are given for maximizing the independence between the components within the solution. This will increase the level of effort required to compromise this solution.

**Table 3. Product Selection Requirements**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-PS-1 | The products used for the Inner and Outer VPN Gateways shall be chosen from the list of IPsec VPN Gateways on the CSfC Components List. | M | T=O | |
| VPN-PS-2 | The products used for the Inner tunnel and Outer tunnel CAs shall either:<br>• be chosen from the list of CAs on the CSfC Components List; or<br>• shall be Enterprise CAs. | M | T=O | |
| VPN-PS-3 | The Inner and Outer VPN Gateways shall either:<br>• come from different manufacturers, where neither manufacturer is a subsidiary of the other; or<br>• be different products from the same manufacturer, where NSA has determined that the products meet the CSfC Program's criteria for implementation independence. | M | T=O | |
| VPN-PS-4 | The Inner and Outer VPN Gateways shall be logically separated using an NSA-approved mechanism. | M | T | VPN-PS-5 |
| VPN-PS-5 | The Inner and Outer VPN Gateways shall be run on physically separate hardware. | M | O | VPN-PS-4 |
| VPN-PS-6 | The Inner and Outer VPN Gateways shall not use the same Operating System (OS). Differences between Service Packs (SP) or version numbers for a particular vendor's OS do not provide adequate diversity. | M | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-PS-7 | The Inner and Outer CAs shall either:<br>• come from different manufacturers, where neither manufacturer is a subsidiary of the other; or<br>• be different products from the same manufacturer, where NSA has determined that the products meet the CSfC Program's criteria for implementation independence. | M | O | optional |
| VPN-PS-8 | The cryptographic libraries used by the Inner and Outer VPN Gateways shall either:<br>• come from different manufacturers, where neither manufacturer is a subsidiary of the other; or<br>• be different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC Program's criteria for implementation independence. | M | O | optional |
| VPN-PS-9 | The cryptographic libraries used by the Inner and Outer CAs shall either:<br>• come from different manufacturers, where neither manufacturer is a subsidiary of the other; or<br>• be different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC Program's criteria for implementation independence. | M | O | optional |
| VPN-PS-10 | Each component that is selected out of the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO/DAA-approved Product Supply Chain Threat Assessment process. (See CNSSD 505 SCRM for additional guidance.) | M | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-PS-11 | Gray Network Firewalls and Inner VPN Gateways shall either:<br>• come from different manufacturers, where neither manufacturer is a subsidiary of the other; or<br>• be two different products from the same manufacturer, where NSA has determined that the two products meet the CSfC Program's criteria for implementation independence. | F | T=O | |
| VPN-PS-12 | Products used for Gray Network Firewalls shall be chosen from the list of Firewalls on the CSfC Components List. | F | T=O | |
| VPN-PS-13 | Inner VPN Gateways and Gray Network Firewalls shall be logically separated using an NSA-approved mechanism. | F | T | VPN-PS-14 |
| VPN-PS-14 | Inner VPN Gateways and Gray Network Firewalls shall be run on physically separate hardware. | F | O | VPN-PS-13 |

It is preferred that the CAs be part of a customer's enterprise keying solution. In that case, the CA will not be selected from the CSfC Components List because it will already exist on the relevant Red or Gray network(s). If there is no existing Enterprise CA, however, the CA used for the solution must also be selected from the CSfC Components List.

# 10 CONFIGURATION REQUIREMENTS

Once the products for the solution are selected, the next step is setting up the components and configuring them in a secure manner. This section consists of generic guidance for how to configure the components of the VPN solution.

## 10.1 OVERALL SOLUTION REQUIREMENTS

**Table 4. Overall Solution Requirements**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-SR-1 | Network services provided by control plane protocols (such as DNS and NTP) to VPN Gateways shall be located on the inside network (i.e., Gray network for Outer VPN Gateways and Red network for Inner VPN Gateways). | M | O | optional |
| VPN-SR-2 | Sites that need to communicate shall ensure that the VPN Gateways selected by each site are interoperable (see Section 4.2). | M | T=O | |
| VPN-SR-3 | The time of day on the Inner VPN Gateways and each infrastructure component within the Red network shall be synchronized with the same time source located in the Red network. | M | T=O | |
| VPN-SR-4 | The time of day on the Outer VPN Gateways and each infrastructure component within the Gray network shall be synchronized with the same time source located in the Gray Management network. | M | T=O | |
| VPN-SR-5 | Default accounts, passwords, community strings, and other default access control mechanisms for all components shall be changed or removed. | M | T=O | |
| VPN-SR-6 | All components shall be properly configured according to local policy and applicable U.S. Government guidance (e.g. Defense Information Systems Agency (DISA) gold disk). In the event of conflict between the requirements in this Capability Package and local policy, this Capability Package takes precedence. | M | T=O | |
| VPN-SR-7 | All physical paths within a Gray network between two Inner VPN Gateways for Red networks of different classification levels shall include an Outer VPN Gateway or a Gray Network Firewall. | M | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-SR-8 | All physical paths within a Gray network between a CA, an Administration Workstation, or a CDP and an Inner VPN Gateway for a Red network whose classification level is lower than the highest classification of data protected by the solution shall include an Outer VPN Gateway or a Gray Network Firewall. | M | T=O | |

## 10.2 CONFIGURATION REQUIREMENTS FOR ALL VPN GATEWAYS

**Table 5. IPsec Encryption (Approved Algorithms up to Top Secret)**

| Security Service | Algorithm Suite 2 | Specifications |
|---|---|---|
| Confidentiality (Encryption) | AES-256 | FIPS PUB 197<br>IETF RFC 6239<br>IETF RFC 6379<br>IETF RFC 6380<br>IETF RFC 6460 |
| Authentication (Digital Signature)<br>(Threshold – Unclassified Only) | RSA 2048 | FIPS PUB 186-4 |
| Authentication (Digital Signature)<br>(Objective)<br>(Threshold – All Classified NSS) | RSA 3072<br>or<br>ECDSA over the curve P-384 with SHA-384 | FIPS PUB 186-4<br>FIPS PUB 186-4<br>IETF RFC 6239<br>IETF RFC 6380<br>IETF RFC 6460 |
| Key Exchange/ Establishment | ECDH over the curve P-384 (DH Group 20)<br>or<br>RSA 3072<br>or<br>DH 3072 | NIST SP 800-56A<br>IETF RFC 6239<br>IETF RFC 6379<br>IETF RFC 6380<br>IETF RFC 6460<br>NIST SP 800-56A |
| Integrity (Hashing) | SHA-384 | FIPS PUB 180-4<br>IETF RFC 6239<br>IETF RFC 6379<br>IETF RFC 6380<br>IETF RFC 6460 |
| Can protect | Up to Top Secret | |

**Table 6. Configuration Requirements for All VPN Gateways**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-CR-1 | The proposals offered by VPN Gateways in the course of establishing the IKE Security Association (SA) and the ESP SA for Inner and Outer Tunnels shall be configured to offer algorithm suite(s) containing only Suite B algorithms (see Table 5). | M | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-CR-2 | Default, self-signed or proprietary device certificates, which are frequently preinstalled by the vendor, for any VPN Gateways shall not be used for establishing SAs. | M | T | VPN-CR-4 |
| VPN-CR-3 | Default, self-signed or proprietary device certificates, which are frequently preinstalled by the vendor, for any VPN Gateways shall be removed. | M | O | VPN-CR-3 |
| VPN-CR-4 | A unique device certificate shall be loaded onto each VPN Gateway along with the corresponding CA (signing) certificate. | M | T=O | |
| VPN-CR-5 | The device certificate shall be used for VPN Gateway authentication during IKE. | M | T=O | |
| VPN-CR-6 | Authentication performed by VPN Gateways shall include a check that device certificates are authorized. This check may use a CRL, OCSP, or a whitelist. | M | T=O | |
| VPN-CR-7 | VPN Gateway authentication with device certificates shall include a check that certificates are not expired. | M | T=O | |
| VPN-CR-8 | The only approved physical paths leaving Red networks shall be through a VPN solution in accordance with this Capability Package or via an NSA-approved solution for protecting data in transit.[1] | M | T=O | |
| VPN-CR-9 | One IPsec tunnel shall use IKEv2 (IETF RFC 5996) key exchange and the other shall use IKEv1 (IETF RFC 2409) key exchange in Main Mode on Phase 1. | M | T | VPN-CR-10 |
| VPN-CR-10 | Both IPsec tunnels shall use IKEv2 (IETF RFC 5996) key exchange. | M | O | VPN-CR-9 |
| VPN-CR-11 | The Inner VPN Gateways shall use protocols and algorithms for creating inner VPN tunnels selected from Table 6 that are approved to protect the highest classification level of the Red network data. | M | T | |

[1] In some cases, the customer will need to communicate with other sites that have NSA-certified Government off-the-Shelf (GOTS) equipment. In particular, it is acceptable for a given site to have both an egress path via an NSA-certified device and an egress path via a layered COTS solution conforming to this Capability Package. This will allow a site to communicate with remote sites that use either solution.

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-CR-12 | The Outer VPN Gateways shall use protocols and algorithms for creating outer VPN tunnels selected from Table 6 that are approved to protect the highest classification level of the Red network data. | M | T | |
| VPN-CR-13 | The VPN Gateways shall use protocols and algorithms for creating all VPN tunnels selected from Algorithm Suite 2 in Table 6. | M | O | VPN-CR-11 and VPN-CR-12 |
| VPN-CR-14 | The VPN Gateways shall use Cipher Block Chaining for IKE encryption. | M | T=O | |
| VPN-CR-15 | The VPN Gateways shall use Cipher Block Chaining for ESP encryption with an HMAC for integrity. | M | T | VPN-CR-16 |
| VPN-CR-16 | The VPN Gateways shall use Galois Counter Mode for ESP encryption. | M | O | VPN-CR-15 |
| VPN-CR-17 | The VPN Gateways shall set the IKE SA lifetime to at most 24 hours. | M | T=O | |
| VPN-CR-18 | The VPN Gateways shall set the ESP SA lifetime to at most 8 hours. | M | T=O | |
| VPN-CR-19 | Inner VPN Gateways shall only authenticate and establish an IPsec tunnel with one another if their Red networks operate at the same security level (as defined in this Capability Package). | M | T=O | |
| VPN-CR-20 | The VPN Gateways shall re-authenticate the identity of the VPN Gateway at the other end of the established tunnel before rekeying the IKE SA. | M | T=O | |

## 10.3 Additional Requirements for Inner VPN Gateways

**Table 7. Additional Requirements for Inner VPN Gateways**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-IR-1 | The Inner VPN Gateway shall use Tunnel mode IPsec or Transport mode IPsec with an associated IP tunneling protocol (e.g. GRE). | M | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-IR-2 | The packet size for packets leaving the external interface of Inner VPN Gateways shall be configured to keep the packets from being fragmented and impacting performance. This requires proper configuration of the Maximum Transmission Unit (MTU) (for IPv4) or Path MTU (PMTU) (for IPv6) and should consider Black network and Outer VPN Gateway MTU/PMTU values to achieve this. | M | O | optional |
| VPN-IR-3 | Inner VPN Gateways shall not allow any packets received on an interface connected to a Red network to bypass encryption and be forwarded out through an interface connected to a Gray network. | M | T=O | |
| VPN-IR-4 | Inner VPN Gateways shall not allow any packets received on an interface connected to a Gray network to bypass decryption and be forwarded out through an interface connected to a Red network. | M | T=O | |

## 10.4 Additional Requirements for Outer VPN Gateways

**Table 8. Additional Requirements for Outer VPN Gateways**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-OR-1 | The Outer VPN Gateway shall use Tunnel mode IPsec. | M | T=O | |
| VPN-OR-2 | Outer VPN Gateways shall not allow any packets received on an interface connected to a Gray network to bypass encryption and be forwarded out through an interface connected to a Black network. | M | T=O | |
| VPN-OR-3 | All traffic received by the Outer VPN Gateway on an interface connected to a Gray network, with the exception of Control Plane traffic, shall have already been encrypted once in accordance with VPN-IR-3, VPN-IR-4, VPN-DM-8, or VPN-DM-19. | M | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-OR-4 | Outer VPN Gateways shall not allow any packets received on an interface connected to a Black network to bypass decryption and be forwarded out through an interface connected to a Gray network. | M | T=O | |

## 10.5 Port Filtering Requirements for VPN Gateways

**Table 9. Port Filtering Requirements for VPN Gateways**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-PF-1 | For all Outer VPN Gateway interfaces connected to a Black network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only IKE, ESP, and control plane protocols (as defined in this Capability Package) approved by organization-defined policy are allowed. | M | T=O | |
| VPN-PF-2 | For all Inner VPN Gateway interfaces connected to a Gray network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only IKE, ESP, and management and control plane protocols (as defined in this Capability Package) approved by organization-defined policy are allowed. | M | T=O | |
| VPN-PF-3 | Traffic filtering rules on the VPN Gateways shall be applied based on known VPN Gateway addresses or address ranges. | M | T=O | |
| VPN-PF-4 | Any service or feature that allows an Outer VPN Gateway to contact a third party server (such as one maintained by the manufacturer) shall be blocked. | M | T | VPN-PF-5 |
| VPN-PF-5 | Any service or feature that allows an Outer VPN Gateway to contact a third party server (such as one maintained by the manufacturer) shall be disabled. | M | O | VPN-PF-4 |
| VPN-PF-6 | Each VPN Gateway shall only accept management traffic on the physical ports connected to its management network. | M | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-PF-7 | Multicast messages received on external interfaces of Outer VPN Gateways shall be dropped. | M | T=O | |
| VPN-PF-8 | For solutions using IPv4, each VPN Gateway shall drop all packets that use IP options. | M | T=O | |
| VPN-PF-9 | For solutions using IPv4, each VPN Gateway shall only accept packets with Transmission Control Protocol (TCP), User Data Protocol (UDP), Encapsulating Security Payload (ESP), or ICMP in the IPv4 Protocol field and drop all other packets. | M | T=O | |
| VPN-PF-10 | For solutions using IPv6, each VPN Gateway shall only accept packets with ESP, TCP, UDP, or ICMPv6 in the IPv6 Next Header field and drop all other packets. | M | T=O | |
| VPN-PF-11 | The Gray network interfaces of Outer VPN Gateways shall allow IKE and IPsec traffic that is between two Inner VPN Gateways protecting networks of the same classification level or that is being used for management of the Gray network. | M | T=O | |
| VPN-PF-12 | The Gray network interfaces of Outer VPN Gateways shall allow HTTP traffic between Inner VPN Gateways and Inner CDPs. | C | T | VPN-PF-13 and VPN-PF-14 |
| VPN-PF-13 | The Gray network interfaces of Outer VPN Gateways shall allow HTTP GET requests from Inner VPN Gateways to Inner CDPs for the URL of the CRL needed by the Inner VPN Gateway, and block all other HTTP requests. | C | O | VPN-PF-12 |
| VPN-PF-14 | The Gray network interfaces of Outer VPN Gateways shall allow HTTP responses from Inner CDPs to Inner VPN Gateways that contain a well-formed CRL per IETF RFC 5280, and block all other HTTP responses. | C | O | VPN-PF-12 |
| VPN-PF-15 | The Gray network interfaces of Outer VPN Gateways shall only permit packets whose source and destination IP addresses match the external interfaces of Inner VPN Gateways that support Red networks of the same classification level. | M | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-PF-16 | The Gray network interfaces of Outer VPN Gateways shall block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface on which the packet was received. | M | T=O | |
| VPN-PF-17 | The Gray network interfaces of Outer VPN Gateways shall allow management and control plane protocols (as defined in this Capability Package) that have been approved by policy. | M | T=O | |
| VPN-PF-18 | The Gray network interfaces of Outer VPN Gateways shall deny all traffic that is not explicitly allowed by requirements VPN-PF-6, VPN-PF-11, VPN-PF-12, VPN-PF-13, or VPN-PF-17. | M | T=O | |

## 10.6 Configuration Change Detection Requirements

**Table 10. Configuration Change Detection Requirements**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-CM-1 | A baseline configuration for all components shall be maintained by the Security Administrator and be available to the Auditor. | M | T=O | |
| VPN-CM-2 | An automated process shall ensure that configuration changes are logged. | M | T=O | |
| VPN-CM-3 | Log messages generated for configuration changes shall include the specific changes made to the configuration. | M | T=O | |

## 10.7 Requirements for Device Management

Only authorized Security Administrators will be allowed to administer the VPN Gateways. The VPN solution will be used as transport for the Secure Shell v2 (SSHv2), IPsec, or TLS data from the Administration Workstation to the VPN Gateway. This means that to remotely administer an Outer VPN Gateway, the existing tunnel between Outer VPN Gateways will carry the SSH, IPsec, or TLS data. In order to remotely administer an Inner VPN Gateway, the SSH, IPsec, or TLS data will travel inside the two tunnels to reach the remote Inner VPN Gateway.

**Table 11. Requirements for Device Management**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-DM-1 | Administration Workstations shall be dedicated for the purposes given in the Capability Package and shall be physically separated from workstations used to manage non-CSfC solutions. | M | T=O | |
| VPN-DM-2 | Administration Workstations shall physically reside within a protected facility where CSfC solution(s) are managed. | M | T=O | |
| VPN-DM-3 | Administration Workstations shall connect from an internal port. Specifically, the Inner VPN Gateway shall be managed from the Red network and the Outer VPN Gateway shall be managed from the Gray network. | M | T=O | |
| VPN-DM-4 | A separate LAN or VLAN on the Red network shall be used exclusively for all management of Inner VPN Gateways and solution components within the Red network. | M | T=O | |
| VPN-DM-5 | A separate LAN or VLAN on the Gray network shall be used exclusively for all management of Outer VPN Gateways and solution components within the Gray network. | M | T=O | |
| VPN-DM-6 | The Gray Management network shall not be directly connected to NIPRNet or any other Unclassified network not dedicated to the administration of CSfC solutions. | M | T=O | |
| VPN-DM-7 | All components shall be configured to restrict the IP address range for the network administration device to the smallest range possible. Note that locally managing solution components is also acceptable. | M | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-DM-8 | All administration of solution components shall be performed from an Administration Workstation<br>• remotely using one of SSHv2, IPsec, or TLS with the appropriate Suite B algorithm selections for the highest classification level of the CSfC solution; or<br>• by managing the solution components locally. | M | T=O | |
| VPN-DM-9 | Security Administrators shall authenticate to solution components before performing administrative functions. | M | T | VPN-DM-10 |
| VPN-DM-10 | Security Administrators shall authenticate to solution components with Suite B compliant certificates before performing administrative functions remotely. | M | O | VPN-DM-9 |
| VPN-DM-11 | Security Administrators shall initiate certificate signing requests for solution components as part of their initial keying within the solution. | M | T=O | |
| VPN-DM-12 | Security Administrators shall initiate certificate revocation prior to disposal of any solution component. | M | T=O | |
| VPN-DM-13 | Administration Workstations that interact with the Certificate Authority for the Outer VPN Gateways must be located on the Gray network. | M | T=O | |
| VPN-DM-14 | VPN Gateways shall obtain certificates through the use of PKCS #10 and #7 requests. | M | T | VPN-DM-15 |
| VPN-DM-15 | Devices shall use Enrollment over Secure Transport (EST) as detailed in IETF RFC 7030 for certificate management. | M | O | VPN-DM-14 |
| VPN-DM-16 | The same Administration Workstation shall not be used to manage both an Inner VPN Gateway and an Outer VPN Gateway. | M | T=O | |
| VPN-DM-17 | Outer VPN Gateways and solution components within the Gray network shall forward log entries to a log server on the Gray Management network within 10 minutes. | M | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-DM-18 | Inner VPN Gateways and solution components within the Red network shall forward log entries to a log server on the Red Management network within 10 minutes. | M | T=O | |
| VPN-DM-19 | All logs forwarded to a log server on the Gray Management network shall be encrypted using SSHv2, IPsec, or TLS with the appropriate Suite B algorithm selections for the highest classification level supported by the solution. | M | T=O | |
| VPN-DM-20 | All logs forwarded to a log server on a Red Management network shall be encrypted using SSHv2, IPsec, or TLS with the appropriate Suite B algorithm selections for the classification level of the Red network. | M | T=O | |
| VPN-DM-21 | Outer VPN Gateways shall only be managed by Security Administrators cleared to at least the highest level of classification of each Red network supported by the Outer VPN Gateway at the physical site the Outer VPN Gateway is located. | M | T=O | |

## 10.8 AUDITING REQUIREMENTS

**Table 12. Auditing Requirements**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-AU-1 | VPN Gateways shall log establishment of a VPN tunnel. | M | T=O | |
| VPN-AU-2 | VPN Gateways shall log termination of a VPN tunnel. | M | T=O | |
| VPN-AU-3 | Solution components shall log all actions performed on the audit log (off-loading, deletion, etc.). | M | T=O | |
| VPN-AU-4 | Solution components shall log all actions involving identification and authentication. | M | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-AU-5 | Solution components shall log attempts to perform an unauthorized action (read, write, execute, delete, etc.) on an object. | M | T=O | |
| VPN-AU-6 | Solution components shall log all actions performed by a user with superuser or administrator privileges. | M | T=O | |
| VPN-AU-7 | Solution components shall log escalation of user privileges. | M | T=O | |
| VPN-AU-8 | Solution components shall log generation, loading, and revocation of certificates. | M | T=O | |
| VPN-AU-9 | Solution components shall log changes to time. | M | T=O | |
| VPN-AU-10 | Solution components shall log when packets received on Gray network interfaces are dropped or blocked. | M | T=O | |
| VPN-AU-11 | The Auditor shall review all logs specified in this Capability Package at least once a week. | M | T=O | |
| VPN-AU-12 | Solution components shall log the results of built-in self-tests. | M | T=O | |
| VPN-AU-13 | Each log entry shall record the date and time of the event. | M | T=O | |
| VPN-AU-14 | Each log entry shall include the identifier of the event. | M | T=O | |
| VPN-AU-15 | Each log entry shall record the type of event. | M | T=O | |
| VPN-AU-16 | Each log entry shall record the success or failure of the event to include failure code, when available. | M | T=O | |
| VPN-AU-17 | Each log entry shall record the subject identity. | M | T=O | |
| VPN-AU-18 | Each log entry shall record the source address for network-based events. | M | T=O | |
| VPN-AU-19 | Each log entry shall record the user and, for role-based events, role identity, where applicable. | M | T=O | |
| VPN-AU-20 | VPN Gateways shall log the failure to download the CRL from a CDP. | C | T=O | |
| VPN-AU-21 | VPN Gateways shall log if the version of the CRL downloaded from a CDP is older than the current cached CRL. | C | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-AU-22 | VPN Gateways shall log if signature validation of the CRL downloaded from a CDP fails. | C | T=O | |
| VPN-AU-23 | A Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) shall be deployed on Gray Management networks to monitor bi-directional traffic between Inner VPN Gateways and Outer VPN Gateways. | M | O | optional |
| VPN-AU-24 | Each IDS in the solution shall be configured in passive mode. | M | O | optional |
| VPN-AU-25 | Each IDS in the solution shall receive data either from a dedicated network tap or via port mirroring from a switch or router within a Gray network. | M | O | optional |
| VPN-AU-26 | The organization shall create IDS rules that generate alerts upon detection of any unauthorized ports or protocols. | M | O | optional |
| VPN-AU-27 | The organization shall create IPS rules that block traffic with unauthorized ports or protocols. | M | O | optional |
| VPN-AU-28 | The organization shall create IDS rules that generate alerts upon detection of any unauthorized destination IP addresses. | M | O | optional |
| VPN-AU-29 | The organization shall create IPS rules that block traffic with any unauthorized destination IP addresses. | M | O | optional |
| VPN-AU-30 | The organization shall establish a baseline of bi-directional network flow data between the Inner VPN Gateway and Outer VPN Gateway. | M | O | optional |
| VPN-AU-31 | The organization shall collect and store bi-directional network flow data between the Inner VPN Gateway and Outer VPN Gateway. | M | O | optional |
| VPN-AU-32 | Auditors shall compare and analyze collected network flow data against the established baseline on at least a weekly basis. | M | O | optional |
| VPN-AU-33 | System Information and Event Management (SIEM) software shall be deployed as the log server on Gray Management networks. | M | O | optional |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-AU-34 | Administrators shall periodically inspect the physical attributes of infrastructure hardware for signs of tampering or other unauthorized changes. | M | O | optional |

## 10.9 Key Management Requirements

### 10.9.1 PKI Requirements for VPN Gateways

**Table 13. PKI Requirements for VPN Gateways**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-KM-1 | The key sizes and algorithms used for Inner and Outer VPN Gateways shall be as specified in Table 5. | M | T=O | |
| VPN-KM-2 | CAs supporting Inner VPN Gateways shall be physically separate from CAs supporting Outer VPN Gateways. | M | T=O | |
| VPN-KM-3 | Both the Inner and Outer tunnel CAs shall operate under a CPS that is formatted in accordance with IETF RFC 3647. | M | T=O | |
| VPN-KM-4 | Both Inner and Outer tunnel PKIs shall use RSA3072 bit or greater within X.509 version 3 certificates. | M | T | VPN-KM-6 |
| VPN-KM-5 | Both Inner and Outer tunnel PKIs shall use ECDSA signatures over curve P-384 with SHA 384 within X.509 version 3 certificates. | M | O | VPN-KM-4 |
| VPN-KM-6 | Inner VPN Gateways shall only trust Inner tunnel CAs used within the solution. | M | T=O | |
| VPN-KM-7 | Outer VPN Gateways shall only trust Outer tunnel CAs used within the solution. | M | T=O | |
| VPN-KM-8 | All public/private key pairs and certificates for VPN Gateways shall be used for authentication only. | M | T=O | |
| VPN-KM-9 | VPN Gateway keys shall not be escrowed. | M | T=O | |
| VPN-KM-10 | The VPN Gateways shall be initially keyed within a physical environment certified to protect the highest classification level of the VPN solution network. | M | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-KM-11 | Rekeying of the VPN Gateways shall be done prior to expiration of keys. | M | T=O | |
| VPN-KM-12 | If rekeying of the VPN Gateways is not completed prior to expiration of keys, they shall be rekeyed through the same process as initial keying. | M | T=O | |
| VPN-KM-13 | Certificate revocation information shall be made available by posting the data to a repository or service that is available for the VPN Gateways. | M | T=O | |
| VPN-KM-14 | New certificates shall be issued as needed in accordance with local policy. | M | T=O | |
| VPN-KM-15 | CAs shall issue an updated CRL within 1 hour of a certificate revocation. | M | T=O | |
| VPN-KM-16 | When a new CRL is issued, the updated CRL shall be distributed to the VPN Gateways within 24 hours. | M | T=O | |
| VPN-KM-17 | CRLs shall expire no later than 31 days after their issue date. | M | T=O | |
| VPN-KM-18 | CRLs shall comply with IETF RFC 5280. | M | T=O | |

### 10.9.2 Enterprise PKI Requirements

**Table 14. Enterprise PKI Requirements**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-KM-19 | Enterprise CAs shall assert a registered Object Identifier (OID) to all of its VPN Gateways. | M | O | optional |
| VPN-KM-20 | Enterprise CAs shall be located on the Red network for Inner VPN Gateways and on the Gray network for Outer VPN Gateways, and be approved to issue certificates (such as one that follows CNSSI 1300 under the NSS PKI Root CA). | M | T=O | |

### 10.9.3 Locally-Run PKI Requirements

**Table 15. Locally-Run PKI Requirements**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-KM-21 | The key validity period for certificates issued by Locally-run CAs shall not exceed 14 months. | M | T=O | |
| VPN-KM-22 | Locally-run CAs shall assert a registered OID to all of its VPN Gateways. | M | T=O | |
| VPN-KM-23 | Locally-run Red network CAs shall only issue certificates to Inner VPN Gateways of CSfC Solutions or to support its own operation. | M | T=O | |
| VPN-KM-24 | Locally-run Gray network CAs shall only issue certificates to Outer VPN Gateways of CSfC Solutions or to support its own operation. | M | T=O | |
| VPN-KM-25 | Locally-run CAs shall issue certificates within a defined and limited name space. | M | T=O | |
| VPN-KM-26 | Locally-run CAs shall issue certificates with unique names. | M | T=O | |

## 10.10 Gray Network Firewall Requirements

**Table 16. Gray Network Firewall Requirements**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-FW-1 | Gray Network Firewalls shall permit IKE and IPsec traffic between two Inner VPN Gateways protecting networks of the same classification level. | F | T=O | |
| VPN-FW-2 | Gray Network Firewalls shall allow HTTP traffic between Inner VPN Gateways and Inner CDPs. | F+C | T | VPN-FW-3 and VPN-FW-4 |
| VPN-FW-3 | Gray Network Firewalls shall allow HTTP GET requests from Inner VPN Gateways to Inner CDPs for the URL of the CRL needed by the Inner VPN Gateway, and block all other HTTP requests. | F+C | O | VPN-FW-2 |
| VPN-FW-4 | Gray Network Firewalls shall allow HTTP responses from Inner CDPs to Inner VPN Gateways that contain a well-formed CRL per IETF RFC 5280, and block all other HTTP responses. | F+C | O | VPN-FW-2 |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-FW-5 | Gray Network Firewalls shall only accept management traffic on the physical ports connected to the Gray Management network. | F | T=O | |
| VPN-FW-6 | Gray Network Firewalls shall only permit packets whose source and destination IP addresses match the external interfaces of Inner VPN Gateways that support Red networks of the same classification level. | F | T=O | |
| VPN-FW-7 | Gray Network Firewalls shall block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface on which the packet was received. | F | T=O | |
| VPN-FW-8 | Gray Network Firewalls shall deny all traffic that is not explicitly allowed by requirements VPN-FW-1, VPN-FW-2, VPN-FW-3, VPN-FW-4, or VPN-FW-5. | F | T=O | |

## 10.11 Requirements for CDP Devices

**Table 17. Requirements for CDP Devices**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-CD-1 | CRLs hosted by CDPs shall not contain extensions other than what is specified in IETF RFC 5280. | C | T=O | |
| VPN-CD-2 | CRLs hosted on Inner CDPs shall be signed by the associated Red Network CA. | C | T=O | |
| VPN-CD-3 | CRLs hosted on Outer CDPs shall be signed by the associated Gray Network CA. | C | T=O | |
| VPN-CD-4 | CDPs shall only issue CRLs over port 80 (HTTP). | C | T=O | |
| VPN-CD-5 | CRLs shall be transferred via an AO-approved one-way transfer mechanism from Red Network CAs to associated Inner CDP servers. | C | T=O | |
| VPN-CD-6 | CRLs shall be transferred via an AO-approved one-way transfer mechanism from Gray Network CAs to associated Outer CDP servers. | C | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-CD-7 | Newly issued CRLs shall be transferred to CDP servers at least 4 days prior to the expiration of the current CRLs. | C | T=O | |
| VPN-CD-8 | VPN Gateways shall attempt to download the latest CRL from a CDP at least once every 24 hours. | C | T=O | |
| VPN-CD-9 | CDPs shall only accept traffic on port 80 and ports used for remote management traffic. | C | T=O | |
| VPN-CD-10 | CDPs shall only accept connections from known VPN Gateway or Administration Workstation addresses or address ranges. | C | T=O | |
| VPN-CD-11 | Red Network CAs shall issue the CRLs for associated Inner CDPs. | C | T=O | |
| VPN-CD-12 | Gray Network CAs shall issue the CRLs for associated Outer CDPs. | C | T=O | |
| VPN-CD-13 | If an integrity check of a CRL pulled from a CDP fails, then VPN Gateways shall use the current cached CRL. | C | T=O | |
| VPN-CD-14 | If a CDP is offline or contains an invalid CRL, then Inner and Outer VPN Gateway CRLs shall be manually updated prior to the expiration of the current CRLs. | C | T=O | |
| VPN-CD-15 | Red Network CAs shall set the CRL Distribution Points extension of the certificates it generates for the VPN solution to the list of URLs hosted by Inner CDPs from which Inner VPN Gateways can download the CRL. | C | T=O | |
| VPN-CD-16 | Gray Network CAs shall set the CRL Distribution Points extension of the certificates it generates for the VPN solution to the list of URLs hosted by Outer CDPs from which Outer VPN Gateways can download the CRL. | C | T=O | |

# 11 REQUIREMENTS FOR SOLUTION OPERATION, MAINTENANCE, AND HANDLING

## 11.1 REQUIREMENTS FOR THE USE AND HANDLING OF SOLUTIONS

The following requirements shall be followed regarding the use and handling of the solution.

**Table 18. Requirements for the Use and Handling of Solutions**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-GD-1 | All components of the solution shall be physically protected as classified devices, classified at the level of the network with the highest classification in the solution or in any other VPN solutions with which it is interconnected. | M | T=O | |
| VPN-GD-2 | Only authorized and appropriately cleared (or escorted) administrators and security personnel shall have physical access to the infrastructure components. | M | T=O | |
| VPN-GD-3 | All components of the solution shall be disposed of as classified devices, unless declassified using AO/DAA-approved procedures. | M | T=O | |
| VPN-GD-4 | Acquisition and procurement documentation shall not include information about how the equipment will be used, to include that it will be used to protect classified information. | M | T=O | |
| VPN-GD-5 | The solution owner shall allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, interviewing) of the solution implementation to ensure it meets the latest version of the Capability Package. | M | T=O | |
| VPN-GD-6 | The AO/DAA will ensure that a compliance audit shall be conducted every year against the latest version of the VPN Capability Package. | M | T=O | |
| VPN-GD-7 | Results of the compliance audit shall be provided to and reviewed by the AO/DAA. | M | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-GD-8 | When a new approved version of the VPN Capability Package is published by NSA, the AO/DAA shall ensure compliance against this new Capability Package within 6 months. | M | T=O | |
| VPN-GD-9 | Solution implementation information, which was provided to NSA during solution registration, shall be updated at least once every 12 months (in accordance with Section 13.3). | M | T=O | |
| VPN-GD-10 | Audit log data shall be maintained for a minimum of 1 year. | M | T=O | |
| VPN-GD-11 | The amount of storage remaining for audit events shall be assessed quarterly in order to ensure that adequate memory space is available to continue recording new audit events. | M | T=O | |
| VPN-GD-12 | Audit data shall be frequently offloaded to a backup storage medium. | M | T=O | |
| VPN-GD-13 | A set of procedures shall be developed by the implementing organization to provide guidance for identifying and reporting security incidents associated with the audit events to the proper authorities and to the data owners. | M | T=O | |
| VPN-GD-14 | The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for determining when the audit log is reaching its maximum storage capacity. | M | T=O | |
| VPN-GD-15 | The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for off-loading audit log data for long- term storage. | M | T=O | |
| VPN-GD-16 | The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for responding to an overflow of audit log data within a product. | M | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-GD-17 | The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for ensuring that the audit log can be maintained during power events. | M | T=O | |
| VPN-GD-18 | Strong passwords shall be used that comply with the requirements of the AO/DAA. | M | T=O | |
| VPN-GD-19 | Security critical patches (such as Information Assurance Vulnerability Alerts (IAVAs)) shall be tested and subsequently applied to all components in the solution in accordance with local policy and this Capability Package. | M | T=O | |
| VPN-GD-20 | Local policy shall dictate how the Security Administrator will install patches to solution components. | M | T=O | |
| VPN-GD-21 | Solution components shall comply with local TEMPEST policy. | M | T=O | |
| VPN-GD-22 | The implementing organization shall complete and submit a VPN CP requirements compliance matrix to their respective AO/DAA. | M | T=O | |
| VPN-GD-23 | All hardware components shall be tracked through an AO-approved inventory management process that identifies each component as part of a CSfC Solution. | M | T=O | |

Additional VPN-GD requirements can be found in Section 12.

### 11.2 Requirements for Incident Reporting

Table 19 lists requirements for reporting security incidents to NSA to be followed in the event that a solution owner identifies a security incident which affects the solution. These reporting requirements are intended to augment, not replace, any incident reporting procedures already in use within the solution owner's organization. It is critical that Security Administrators (SAs), Certificate Authority Administrators (CAAs), and Auditors are familiar with maintaining the solution in accordance with this Capability Package. Based on familiarity with the known-good configuration of the solution, personnel responsible for the operations and maintenance of the solution will be better equipped to identify reportable incidents.

For the purposes of incident reporting, "malicious" activity includes not only events that have been attributed to activity by an adversary but also any events that are unexplained. In other words, an activity is assumed to be malicious unless it has been determined to be the result of known non-malicious activity.

Table 19 only provides requirements directly related to the incident reporting process. See Section 10.8 for requirements supporting the detection of events that may reveal that a reportable incident has occurred.

**Table 19. Incident Reporting Requirements**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-RP-1 | Solution owners shall report confirmed incidents meeting the criteria in VPN-RP-3 through VPN-RP-13 within 24 hours of detection via JIMS or contacting NSA as specified in the CSfC Registration Letter issued for the solution. | M | T=O | |
| VPN-RP-2 | At a minimum, the organization shall provide the following information when reporting security incidents:<br>• CSfC Registration Number<br>• Point of Contact (POC) name, phone, email<br>• Alternate POC name, phone, email<br>• Classification level of affected solution<br>• Name of affected Network(s)<br>• Affected component(s) manufacturer/vendor<br>• Affected component(s) model number<br>• Affected component(s) version number<br>• Date and time of incident<br>• Description of incident<br>• Description of remediation activities<br>• Is Technical Support from NSA requested? (Yes/No) | M | T=O | |
| VPN-RP-3 | Solution owners shall report a security failure in any of the CSfC solution components. | M | T=O | |
| VPN-RP-4 | Solution owners shall report any evidence of a compromise or spillage of classified data caused by a failure of the CSfC Solution. | M | T=O | |

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-RP-5 | For all Gray Network interfaces, solution owners shall report any malicious inbound and outbound traffic. | M | T=O | |
| VPN-RP-6 | Solution owners shall report any evidence of an unauthorized device/user gaining access to the classified network via the solution. | M | T=O | |
| VPN-RP-7 | Solution owners shall report if a solution component sends traffic with an unauthorized destination address. | M | T=O | |
| VPN-RP-8 | Solution owners shall report any malicious configuration changes to the components. | M | T=O | |
| VPN-RP-9 | Solution owners shall report any unauthorized escalation of privileges to any of the CSfC solution components. | M | T=O | |
| VPN-RP-10 | Solution owners shall report any evidence of malicious physical tampering with solution components. | M | T=O | |
| VPN-RP-11 | Solution owners shall report any evidence that one or both of the layers of the solution failed to protect the data. | M | T=O | |
| VPN-RP-12 | Solution owners shall report any significant degradation of services provided by the solution. | M | T=O | |
| VPN-RP-13 | Solution owners shall report malicious discrepancies in the number of VPN connections established by Outer VPN Gateways and by Inner VPN Gateways. | M | T=O | |

# 12 ROLE-BASED PERSONNEL REQUIREMENTS

The roles required to administer and maintain the solution are defined below, along with doctrinal requirements for these roles.

**Security Administrator** – The Security Administrator shall be responsible for maintaining, monitoring, and controlling all security functions for the entire suite of products composing the VPN solution. Security Administrator duties include but are not limited to:

1) Ensuring that the latest security-critical software patches and updates (such as IAVAs) are applied to each product.

2) Documenting and reporting security-related incidents to the appropriate authorities.

3) Coordinating and supporting product logistic support activities including integration and maintenance. Some logistic support activities may require that the Security Administrator escort uncleared personnel.

4) Employing adequate defenses of auxiliary network devices to enable proper and secure functionality of the VPN solution.

5) Ensuring that the implemented VPN solution remains compliant with the latest version of this Capability Package.

**Certificate Authority Administrator (CAA)** – The CAA shall be responsible for maintaining, monitoring, and controlling all security functions for the CA products. CAA duties include but are not limited to:

1) Administering the CA, including authentication of all components requesting certificates.

2) Maintaining and updating the CRL.

**Auditor** – The Auditor shall be responsible for reviewing the actions performed by the Security Administrator and CAA and events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the VPN solution. Auditor duties include but are not limited to:

1) Reviewing, managing, controlling, and maintaining security audit log data.

2) Documenting and reporting security-related incidents to the appropriate authorities.

3) The Auditor will only be authorized access to Outer and Inner administrative components.

**Solution Integrator** – In certain cases, an external integrator may be hired to implement a VPN solution based on this Capability Package. Solution Integrator duties may include but are not limited to:

1) Acquiring the products that compose the solution.

2) Configuring the VPN solution in accordance with this Capability Package.

3) Documenting, testing, and maintaining the solution.

4) Responding to incidents affecting the solution.

Additional policies related to the personnel that perform these roles in a VPN Solution are as follows:

**Table 20. Role-Based Personnel Requirements**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-GD-24 | The Security Administrator, CAAs, Auditor, Remote User, and Solution Integrators shall be cleared to the highest level of data protected by the VPN solution. When an Enterprise CA is used in the solution, the CAA already in place may also support this solution, provided they meet this requirement. | M | T=O | |
| VPN-GD-25 | The Security Administrator, CAA, and Auditor roles shall be performed by different people. | M | T=O | |
| VPN-GD-26 | All Security Administrators, CAAs, Remote Users, and Auditors shall meet local information assurance training requirements. | M | T=O | |
| VPN-GD-27 | The CAA(s) for the Inner tunnel shall be different individuals from the CAA(s) for the Outer tunnel. | M | T=O | |
| VPN-GD-28 | The Security Administrator(s) for the Inner VPN Gateways and supporting components on Red networks shall be different individuals from the Security Administrator(s) for the Outer VPN Gateways and supporting components on Gray networks. | M | O | optional |

# 13 INFORMATION TO SUPPORT AO/DAA

This section details items that likely will be necessary for the customer to obtain approval from the system AO/DAA. The customer and AO/DAA have obligations to perform the following:

- The customer, possibly with support from a System Integrator, instantiates a solution implementation that follows the NSA-approved Capability Package.
- The customer has a testing team develop a Test Plan and perform testing of the VPN solution, see Section 13.1.
- The customer has system certification and accreditation performed using the risk assessment information referenced in Section 13.2.

- The customer provides the results from testing and system certification and accreditation to the AO/DAA for use in making an approval decision. The AO/DAA is ultimately responsible for ensuring that all requirements from the Capability Package have been properly implemented in accordance with the CP.
- The customer registers the solution with NSA and re-registers yearly to validate its continued use as detailed in Section 13.3.
- Customers who want to use a variant of the solution detailed in this Capability Package will contact their NSA/IAD Client Advocate to determine ways to obtain NSA approval.
- The AO/DAA will ensure that a compliance audit shall be conducted every year against the latest version of the VPN Capability Package, and the results shall be provided to the AO/DAA.
- The AO/DAA will ensure that certificate revocation information is updated on all the VPN Gateways in the solution in the case of a compromise.
- The AO/DAA will ensure that any Layer 2 or Layer 3 control plane protocols that are used in the solution are necessary for the operation of the network and that local policy supports their use.
- The AO/DAA will report incidents affecting the solution in accordance with Section 11.2.

The system AO/DAA maintains configuration control of the approved solution implementation over the lifecycle of the solution. Additionally, the AO/DAA shall ensure that the solution remains properly configured with all required security updates implemented.

## 13.1 Solution Testing

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of a VPN solution. This T&E will be a critical part of the approval process for the AO/DAA, providing a robust body of evidence that shows compliance with this Capability Package.

The security features and operational capabilities associated with the use of the solution shall be tested. The following is a general high-level methodology for developing the test plan and procedures and for the execution of those procedures to validate the implementation and functionality of the VPN solution. The entire solution, to include each component described in Section 5, is addressed by this test plan.

1) Set up the baseline network and configure all components.
2) Document the baseline network configuration. Include product model and serial numbers, and software version numbers at a minimum.

3) Develop a Test Plan for the specific implementation using the test requirements from Section 14. Any additional requirements imposed by the local AO/DAA should also be tested, and the Test Plan shall include tests to ensure that these requirements do not interfere with the security of this solution as described in this Capability Package.

4) Perform testing using the test plan derived in Step 3. Network testing will consist of both Black Box testing and Gray Box testing. A two-person testing approach should be used to administer the tests. During test execution, security and non-security related discrepancies with the solution shall be documented.

5) Compile findings, to include comments and vulnerability details as well as possible countermeasure information, into a Final Test Report to be delivered to the AO/DAA for approval of the solution.

The following testing requirement has been developed to ensure that the VPN solution functions properly and meets the configuration requirements from Section 10. Testing of these requirements should be used as a minimum framework for the development of the detailed test plan and procedures.

**Table 21. Test Requirements**

| Req # | Requirement Description | Capabilities | Threshold / Objective | Alternative |
|---|---|---|---|---|
| VPN-TR-1 | The organization implementing the Capability Package shall perform all tests listed in Section 14. | M | T=O | |

## 13.2 Risk Assessment

The risk assessment of the VPN solution presented in this Capability Package focuses on the types of attacks that are feasible against this solution and the mitigations that can be employed. Customers should contact their NSA/IAD Client Advocate to request this document, or visit the Secret Internet Protocol Router Network (SIPRNet) CSfC site for information. The process for obtaining the risk assessment is available on the SIPRNet CSfC website. The AO/DAA shall be provided a copy of the NSA risk assessment for their consideration in approving the use of the solution.

## 13.3 Registration of Solutions

All customers using CSfC solutions to protect information on National Security Systems shall register their solution with NSA prior to operational use. This registration will allow NSA to track where VPN Capability Package solutions are instantiated and to provide the AO/DAAs at those sites with appropriate information, including any significant vulnerabilities that may be discovered in components or high-level designs approved for these solutions. The CSfC solution registration process is available at http://www.nsa.gov/ia/programs/csfc_program.

Solution registrations are valid for one year from the date the solution registration is approved, at which time customers are required to re-register their solution in order to continue using it. Approved Capability Packages will be reviewed twice a year, or as events warrant. Registered users of this Capability Package will be notified when an updated version is published. When a new version of this Capability Package that has been approved by the IAD Director is published, customers will have six months to bring their solutions into compliance with the new version of the Capability Package and re-register their solution (see requirement VPN-GD-8). Customers are also required to update their registrations whenever the information provided on the registration form changes.

# 14 TESTING REQUIREMENTS

This section contains the specific tests that allow the Security Administrator or System Integrator to ensure they have properly configured the solution. As defined in Section 8, in order to comply with this Capability Package, a solution must at minimum implement all Threshold requirements associated with each of the capabilities it supports, and should implement the Objective requirements associated with those capabilities where feasible. These tests may also be used to provide evidence to the AO/DAA regarding compliance of the solution with this Capability Package. Note that the details of the procedures are the responsibility of the final developer of the solution test plan in accordance with AO/DAA-approved network procedures. The AO/DAA is ultimately responsible for ensuring that all requirements from the Capability Package have been properly implemented.

## 14.1 PRODUCT SELECTION

This section contains a procedure to verify that the components in this CP were selected to ensure independence in several important features.

**Requirements being tested**: VPN-PS-1 through VPN-PS-12, VPN-SR-2,

**Procedure Description:**

1) For each VPN Gateway, perform the following:

    a) Verify that the Inner and Outer VPN Gateways are on the list of IPsec VPN Gateways on the CSfC Components List. (VPN-PS-1)

    b) Verify that the Inner and Outer VPN Clients are on the list of IPsec VPN Clients on the CSfC Components List. (VPN-PS-1)

    c) Verify that the Inner and Outer VPN Gateways either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (VPN-PS-3)

d) Verify the Inner and Outer VPN Gateways are logically separated using an NSA-approved mechanism. (VPN-PS-4)

e) Verify the Inner and Outer VPN Gateways are running on physically separate hardware platforms. (VPN-PS-5)

f) Verify the Inner and Outer VPN Gateways are running differing Operating Systems. (VPN-PS-6)

g) Verify that the cryptographic libraries used by the Inner and Outer VPN Gateways either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (VPN-PS-8)

2) For each CA, perform the following:

a) Verify the Inner and Outer tunnel CAs came from the list of CAs on the CSfC Components List or are Enterprise CAs. (VPN-PS-2)

b) Verify that the Inner and Outer CAs either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (VPN-PS-7)

c) Verify that the cryptographic libraries used by the Inner and Outer CAs either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (VPN-PS-9)

3) For each Gray Network Firewall and Inner VPN Gateway, perform the following:

a) Verify that the Gray Network Firewalls and Inner VPN Gateways either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (VPN-PS-11)

4) For each Gray Network Firewall, perform the following:

a) Verify that the Gray Network Firewalls are on the list of Firewalls on the CSfC Components List. (VPN-PS-12)

5) For all components used, review the mitigations in the Product Supply Chain Threat Assessment. Ensure that mitigations identified in the assessment are implemented according to the implementing organization's AO/DAA-approved Product Supply Chain Threat Assessment process. (VPN-PS-10)

6) For sites requiring interoperability, ensure that VPN Gateways selected for each tunnel can be configured to communicate using the requirements specified in this Capability Package. (VPN-SR-2)

**Expected Result:**

The results of the inspection should reveal that the VPN Solution components conform to the VPN CP.

## 14.2 Physical Layout of Solution

This section contains a procedure to create an accurate record of the physical components composing the VPN solution (including workstations, VPN Gateways, CAs, and wiring). The test will also ensure that the physical implementation of the VPN solution matches one of the high-level designs given in the VPN Capability Package.

**Requirements being tested**:, VPN-CR-8

**Procedure Description:**

1) Ensure there are no wireless or physical connections to the solution that are not included in this Capability Package, which may allow for traffic to leave a Red or Gray network in a manner that does not go through the VPN solution (or an NSA-certified encryptor). (VPN-CR-8)

**Expected Result:**

For Step 1, there should be no extraneous wireless or physical connections allowing data to leave Red or Gray networks besides through the VPN solution (or an NSA-certified encryptor). For Step 2, Gray Management network traffic should be separate from Gray network traffic. For Step 3, network services should be located inside the network.

## 14.3 VPN Gateway Configurations

This section contains a procedure to ensure that the configurations for all the VPN Gateways in the VPN solution follow the requirements given in this Capability Package.

**Requirements being tested**: VPN-SR-3, VPN-SR-4, VPN-SR-7, VPN-SR-8, VPN-CR-1, VPN-CR-3 through VPN-CR-8, VPN-CR-11, VPN-CR-12, VPN-CR-15 through VPN-CR-20, VPN-IR-1 through VPN-IR-4, VPN-OR-1 through VPN-OR-4, VPN-PF-1 through VPN-PF-18, VPN-DM-1 through VPN-DM-16, VPN-KM-7, VPN-KM-8

**Procedure Description:**

1) For each VPN Gateway in the solution, perform the following:

   a) Obtain the current configuration for the VPN Gateway.

   b) Verify a unique device certificate is loaded with the corresponding CA signing certificate. (VPN-CR-4)

c) Verify a device certificate from a CA included in the VPN solution is listed in the configuration for authentication. (VPN-CR-5)

d) Ensure the corresponding CA signing certificate and certificate revocation information are on the VPN Gateway. (VPN-CR-6)

e) Ensure the corresponding CA signing certificate and certificate revocation information are on the VPN Component. (VPN-CR-7)

f) Verify the requirements VPN-CR-1, VPN-CR-3, VPN-CR-4, VPN-CR-8, VPN-CR-11, VPN-CR-12, VPN-CR-15 through VPN-CR-20, VPN-PF-1 through VPN-PF-4, VPN-PF-8, VPN-PF-10, VPN-PF-11, VPN-PF-12, VPN-SR-7, and VPN-SR-8 are configured properly.

g) Ensure the time of day matches the current time. This should be within a small margin of error, to be determined by the AO/DAA. (VPN-SR-3, VPN-SR-4)

h) Verify that the VPN Gateways are configured to re-authenticate the identity of the VPN Gateways at the other end before rekeying the IKE SA. (VPN-CR-20)

2) For each Inner VPN Gateway in the solution, use the configuration from 1a and perform the following:

a) Log into the Inner VPN Gateways and verify that they are configured to use Tunnel or Transport mode IPsec with an associated IP Protocol (e.g. GRE). (VPN-IR-1)

b) Log into the Inner VPN Gateways and verify that the MTU (for IPv4) or the PMTU (for IPv6) has been configured to an appropriate size. (VPN-IR-2)

c) Using a packet analyzer tool on the Inner VPN Gateway, verify that traffic leaving the external interface going to the Outer VPN Gateway is encrypted. (VPN-IR-3)

d) Using a packet analyzer tool on the Inner VPN Gateway, verify that traffic coming through the external interface of the Inner VPN Gateway is decrypted. (VPN-IR-4)

e) Verify all CA signing certificates used for these components are from Inner tunnel CAs. (VPN-KM-7)

f) Verify that requirement VPN-DM-4 is configured and using a packet sniffer, inspect traffic within the Red Network. (VPN-DM-4)

g) Verify that the Inner VPN Gateway is configured to only authenticate and establish an IPsec tunnel with another Inner VPN Gateway that is at the same security level as defined in the Capability Package. (VPN-CR-19)

3) For each Outer VPN Gateway in the solution, use the configuration from 1a and perform the following:

   a) Log into the Outer VPN Gateways and verify that they are configured to use Tunnel mode IPsec. (VPN-OR-1)

   b) Verify the requirements VPN-OR-2, VPN-OR-3, VPN-PF-4, VPN-PF-5, VPN-PF-7, and VPN-PF-11 through VPN-PF-18 have been properly configured.

   c) Verify that requirement VPN-DM-5 is configured and using a packet sniffer, inspect traffic within the Gray Network. (VPN-DM-5)

   d) Using a packet analyzer tool on the Outer VPN Gateway, verify that traffic coming through the external interface of the Outer VPN Gateway is decrypted. (VPN-OR-4)

   e) Verify that all CA signing certificates used for these components are from Outer tunnel CAs. (VPN-KM-8)

4) Ensure the configuration files state that all communications between Outer VPN Gateways and any third party servers are blocked. (VPN-PF-4)

5) Ensure the configuration files state that all communications between Outer VPN Gateways and any third party servers are disabled. (VPN-PF-5)

6) For all device administration, verify that requirements VPN-DM-1, VPN-DM-2, VPN-DM-3, VPN-DM-7, VPN-DM-8, and VPN-SR-6 are configured properly.

7) For each administration workstation, ensure the Security Administrator is required to authenticate to the component before being granted access. (VPN-DM-9)

8) For each administration workstation, ensure the Security Administrator is required to authenticate to solution components using Suite B compliant certificates. (VPN-DM-10)

9) Ensure that certificate signing requests are initiated by the Security Administrator as part of their initial keying within the solution. (VPN-DM-11)

10) Ensure that certificate revocations are initiated by the Security Administrator prior to disposal of any solution component. (VPN-DM-12)

11) Ensure that Administration Workstations that interact with the Certificate Authority for the Outer VPN Gateways is located on the Gray Network. (VPN-DM-13)

12) Ensure that VPN Gateways obtain certificates through the use of PKCS#10 and #7 requests. (VPN-DM-14)

13) Ensure that devices use EST as detailed in RFC 7030 for certificate management. (VPN-DM-15)

14) Ensure that the same Administration Workstation is not used to manage both Inner and Outer VPN Gateways. (VPN-DM-16)

15) Ensure that requirement VPN-DM-6 has been configured properly.

**Expected Result:**

For Steps 1-7, all VPN Gateways should be configured properly according to the requirements found in this Capability Package. For Steps 8-10, all VPN Gateway administration devices should be configured properly based upon the requirements of this Capability Package. For Steps 11-17, all of the procedures have been followed or are in place.

## 14.4 CA CONFIGURATIONS

This section contains a procedure to ensure that the configurations for all of the CAs used within the VPN solution follow the requirements given in this Capability Package.

**Requirements being tested**: VPN-KM-1 through VPN-KM-6, VPN-KM-10 through VPN-KM-12, VPN-KM-13 through VPN-KM-23, VPN-KM-25

**Procedure Description:**

1) Verify the requirements VPN-KM-1 through VPN-KM-6, and VPN-KM-10 are met by both Inner tunnel CAs and Outer tunnel CAs.

2) Verify that any Inner tunnel CAs and Outer tunnel CAs which are a Enterprise CAs meet the requirements VPN-KM-20 and VPN-KM-21.

3) Verify the requirements VPN-KM-22 through VPN-KM-26 are met by any Locally-run CAs.

4) Verify the VPN Gateways were keyed in a manner consistent with VPN-KM-11, VPN-KM-12, VPN-KM-17, and VPN-KM-13.

5) Ensure that the required certificate revocation information and CA signing certificates are present on each VPN Gateway. (VPN-KM-14)

6) Review the implementing organization's policy for how new certificates are to be issued. As a Certificate Authority Administrator, issue a certificate for a new user in accordance with the policy. (VPN-KM-15)

**Expected Result:**

For Steps 1-6, all CAs should be configured to meet the requirements being tested from Section 10.10 of this Capability Package.

## 14.5 CRL Requirements for CAs

This section contains procedures for ensuring that policy is in place for CA CRLs.

**Requirements being tested:** VPN-KM-16 through VPN-KM-19

**Procedure Description:**

1) Verify that the implementing organization has an approved policy in place that states that the CA shall generate an updated CRL within 1 hour of a certificate revocation. (VPN-KM-16)

2) Verify that the implementing organization has an approved policy in place that states that when a certificate is revoked, the updated CRL shall be distributed to the VPN Gateways within 24 hours of revocation. (VPN-KM-17)

3) Verify that the implementing organization has an approved policy in place that states that CRLs shall expire no later than 31 days after their issue date. (VPN-KM-18)

4) Verify that the information contained within the CRL complies with IETF RFC 5280. (VPN-KM-19)

    a) Pull down a valid CRL from the Red Network CAs and Gray Network CAs.

    b) Verify that the information contained within the CRL complies with IETF RFC 5280.

**Expected Result:**

For Steps 1-3, the implementing organization should have policies in place to address the requirements identified. For step 4, CRL information will comply with IETF RFC 5280.

## 14.6 Use of Certificates from Trusted CAs

This section contains a procedure to ensure that public/private keys and certificates are only used for authentication from trusted CAs.

**Requirements being tested**: VPN-DM-17, VPN-DM-18, VPN-AU-8, VPN-KM-9

**Procedure Description:**

1) Ensure that the solution is in its default setting and that the VPN connections are established when the proper certificates (see Section 6) are used to authenticate the VPN Gateways.

2) Install approved certificates, generated by the approved CAs, on the VPN Gateways and configure the solution so that one of the VPN Gateways uses this certificate for authentication. (VPN-KM-9)

   a) Verify an entry to the Audit log has been created due to certificate loading. (VPN-AU-8)

   b) Start the VPN connections using the new configuration.

   c) Verify the connection is successful and that end-to-end communication is provided because the Gateways will authenticate. Verify that this success is logged in the audit data.

   d) Repeat this test for each VPN Gateway.

3) When testing is complete remove the alternate certificates and return the configuration to its proper settings. Verify that an entry to the Audit log has been created due to certificate deletion and the log is sent to the centralized host. (VPN-AU-8, VPN-DM-17, VPN-DM-18)

**Expected Result:**

Authentication will occur when the VPN Gateways identify the trust anchor of the certificates, provided the solution is configured correctly. All results are expected to be pass/fail.

### 14.7 Use of Revoked Certificates

This section contains a procedure to ensure that only valid certificates are accepted. This section focuses on certificates that have been revoked (and are therefore invalid) and does not include all types of validity testing.

**Requirements being tested**: VPN-AU-8, VPN-AU-10, VPN-KM-7, VPN-KM-8, VPN-KM-14

**Procedure Description:**

1) Ensure the solution is in its default setting and that the VPN connections are established when valid certificates (see Section 6) are used to authenticate the VPN Gateways.

2) Revoke a certificate for one of the VPN Gateways (or install an alternate revoked certificate on one of the VPN Gateways), and ensure the solution is configured so that this revoked certificate will be used for authentication.

   a) If applicable, verify that an entry to the Audit log has been created due to certificate loading. (VPN-AU-8)

   b) Ensure the VPN Gateways contain the latest certificate revocation information to include the revoked certificate to be used for authentication. (VPN-KM-14)

   c) Start the VPN connection.

d) Verify that the connection is not successful and that end-to-end communication is not provided because the Gateways will fail to authenticate the revoked certificate. Verify that this failure is logged in the audit data. (VPN-KM-7, VPN-KM-8, VPN-AU-10)

e) Repeat this test for each VPN Gateway; only one VPN Gateway should offer the revoked certificate per connection.

3) When testing is complete remove the revoked certificates and return the configuration to its proper settings. Verify that an entry to the Audit log has been created due to certificate deletion. (VPN-AU-8)

**Expected Result:**

Authentication will not occur when the VPN Gateways cannot verify the validity of the certificates, provided the solution is configured correctly. All results are expected to be pass/fail.

## 14.8 Configuration Change Detection

This section contains a procedure to ensure that changes made to any of the VPN Gateway configurations are detected by the Configuration Change Detection tool.

**Requirements being tested**: VPN-CM-1 through VPN-CM-3

**Procedure Description:**

1) The following steps shall be performed for each of the VPN Gateways within the solution.

a) Log into the VPN Gateway.

b) Compare the current version of the VPN Gateway configuration with the stored baseline and ensure the current version matches the stored configuration. (VPN-CM-1)

c) Make a change to the configuration, preferably something that is not fundamental to the security of the VPN solution.

d) Look in the audit log to determine if a log entry has been generated about the configuration change and that the changes from 1c are recorded. (VPN-CM-2, VPN-CM-3)

**Expected Result:**

The Auditor will validate the baseline configuration was stored in Step 1b. In Step 1d, there should be a log entry created for the configuration change in the audit log including the actual configuration change.

## 14.9 AUDIT

This section contains procedures for ensuring audit events are detected, the proper information is logged for each event, and there is a procedure detailed in the CPS documentation for auditing each CA device.

**Requirements being tested**: VPN-AU-1 through VPN-AU-7, VPN-AU-9, VPN-AU-11 through VPN-AU-19, VPN-AU-21 through VPN-AU-34, VPN-KM-3, VPN-DM-17 through VPN-DM-20

**Procedure Description:**

1) Examples for testing the ability of each VPN Gateway to audit and log audit events specified in the CP are given below. Verify that for each event logged, the applicable data regarding the event is recorded for the log entry in accordance with Section 10.9.

    a) All actions performed by a user with superuser privileges (auditor, administrator, etc.) and any escalation of user privileges. (VPN-AU-6, VPN-AU-7)

        i) Log in as an administrator to the VPN Gateway .

        ii) Perform a variety of administrator actions on the VPN Gateway .

        iii) Verify a log entry was created for each action taken in Step ii that required superuser privileges and also states the escalation of privileges.

        iv) Revert back to the baseline configuration, eliminating the changes made in Step ii.

        v) Repeat the above with the Auditor role.

    b) Changes to time. (VPN-AU-9, VPN-AU-19)

        i) Log in as a Security Administrator to the VPN Gateway.

        ii) Modify the system time on the VPN Gateway by at least 1 hour.

        iii) Verify a log entry was created due to the change in system time and by whom.

        iv) Revert the system time back to the accurate time of day.

    c) Log into and out of the VPN Solution as a normal user and send traffic to the Red Network. Then log into the central log server as an Auditor, and inspect the audit entry for the following: (VPN-DM-17, VPN-DM-18)

        i) Verify that the log on as a normal user is logged and has an identifiable code for the type of event. (VPN-AU-4, VPN-AU-15)

ii) Verify that the log entry identifies the subject accessing the solution. (VPN-AU-17)

iii) Verify that the log entry identifies the event. (VPN-AU-14)

iv) Verify that the log entry includes the time, date, and the time zone offset. (VPN-AU-13)

d) Establish and terminate a VPN tunnel. Verify in the logs, that these two events were logged. (VPN-AU-1, VPN-AU-2)

e) Ensure all built-in self-test results have been recorded in the audit log which may indicate failures in cryptographic functionality. (VPN-AU-12)

i) Completely power down the VPN Gateway.

ii) Power the VPN Gateway back up so that the automatic self-tests are run.

iii) Verify a log entry was created due to running the self-tests.

f) Log into a VPN Gateway as a Security Administrator and delete previously recorded audit log. Verify the log recorded this deletion. (VPN-AU-3)

g) As the Certificate Administrator, log into the audit log and attempt to delete a log entry. Verify this action is recorded with a failure code. (VPN-AU-5, VPN-AU-16)

h) Verify a log entry was created for the attempted unauthorized action.

2) Verify the source address for all audit log entries is recorded. (VPN-AU-18)

3) Verify there is a procedure detailed in the CPS documentation for auditing each CA device within the solution. (VPN-KM-3)

4) Inspect the organization's implementing policy to verify that it states that audit logs shall be monitored by the Auditor at least weekly. (VPN-AU-11)

5) Verify that all logs forwarded to a log server on a Gray Management network are configured to be encrypted while in transit using SSHv2, IPSEC, or TLS with the appropriate Suite B algorithm supported by the solution. (VPN-DM-19)

6) Verify that all logs forwarded to a log server on a Red Management network are configured to be encrypted while in transit using SSHv2, IPSEC, or TLS with the appropriate Suite B algorithm supported by the solution. (VPN-DM-20)

7) Verify that the procedures VPN-AU-23, VPN-AU-24 and have been implemented and are configured properly.

8) Verify that the procedures VPN-AU-26 through VPN-AU-35 are currently in place by the implementing organization and are followed.

**Expected Result:**

For Step 1, all occurrences of auditable events given should generate an entry in the audit log. For Step 2, the source address should be the VPN Gateway's loopback address. For Step 3, there should be a procedure for auditing the CA devices in the solution outlined in the CPS document. For Step 4, ensure the implementing organization has a policy that complies with this requirement. For Steps 5-6, all logs forwarded on Red Management and Gray Management networks should be encrypted with the appropriate protocols. For Steps 7-8, all procedures have been followed and are in place.

## 14.10 Implementation of Guidance

This section ensures there are procedures in place and/or that procedures were followed regarding the procurement of products and use of the VPN solution. It also ensures the personnel are in place to manage and administer this solution following the guidelines given in the Capability Package.

**Requirements being tested**: VPN-KM-17, VPN-GD-1 through VPN-GD-28, VPN-DM-21

**Procedure Description:**

1) Verify the procedures given in VPN-GD-1 through VPN-GD-4, VPN-GD-9 through VPN-GD-23, VPN-KM-17 and VPN-DM-21 were/are followed and/or are currently in place.

2) Verify the solution owner understands that he/she shall allow and fully cooperate with an NSA-ordered IA compliance audit of this solution implementation. (VPN-GD-5)

3) Verify the solution owner and AO/DAA are aware that a compliance audit will be conducted every year. (VPN-GD-6)

4) Verify the AO/DAA is aware that they shall receive the results of the compliance audit and are responsible for reviewing the completed audit. (VPN-GD-7)

5) Verify the solution owner and AO/DAA are aware that when new versions of the VPN Capability Package are published by NSA they will have 6 months to bring their solution into compliance with this new version of the Capability Package. (VPN-GD-8)

6) Verify the solution owner and AO/DAA are aware that they shall provide updated solution information to NSA on a yearly basis. (VPN-GD-9)

7) Verify the personnel requirements given in VPN-GD-24 through VPN-GD-27 are met by the personnel supporting this implementation of the VPN solution.

8) Verify that no individual is both the Security Administrator for the Inner VPN Gateways and supporting components on Red networks and the Security Administrator for the Outer VPN Gateways and supporting components on Gray networks. (VPN-GD-28)

**Expected Result:**

For Steps 1-9, all of these procedures have been followed or are in place.

## 14.11 Solution Functionality

This section contains a procedure for ensuring the implementing organization complies with the testing requirements.

**Requirements being tested:** VPN-TR-1

**Procedure Description:**

1) The implementing organization's DAA will inspect the test report in order to ensure all testing requirements have been met. (VPN-TR-1)

**Expected Result:**

The report will ensure the implementing organization complies with the VPN Solution.

## 14.12 Gray Network Firewall Placement

This section contains a procedure for ensuring that the placement of Gray Network Firewalls within the solution complies with the requirements of this Capability Package.

**Requirements being tested:** VPN-PS-13, VPN-PS-14, VPN-SR-7, VPN-SR-8

**Procedure Description:**

1) For each Gray Network Firewall within the solution:

   a) Verify that it is logically separated from any Inner VPN Gateways running on the same physical hardware using an NSA-approved separation mechanism. (VPN-PS-13)

   b) Verify that it is running on physically separate hardware from any Inner VPN Gateways. (VPN-PS-14)

2) For each Inner VPN Gateway within the solution:

   a) Verify that every physical path through a Gray network between it and another Inner VPN Gateway for a Red network of a different classification level contains at least one Outer VPN Gateway or Gray Network Firewall. (VPN-SR-7)

b) If Inner VPN Gateways protect a Red network of a classification level lower than the highest classification level protected by the overall system, verify that every physical path through the Gray network and a Certificate Authority, Administration Workstation, or CDP contains at least one Gray Network Firewall. (VPN-SR-8)

**Expected Result:**

In Step 1, the Inner VPN Gateways and Gray Network Firewalls are verified to be separate physical devices. In Step 2, Gray Network Firewalls are verified to be placed at all appropriate positions within the Gray network.

## 14.13 Gray Network Firewall IPsec Filtering Rules

This section contains a procedure for ensuring that the filtering rules on Gray Network Firewalls are configured so that the only IPsec traffic allowed through the firewall is between Inner VPN Gateways that are allowed to establish VPN tunnels with one another.

**Requirements being tested:** VPN-AU-10, VPN-FW-1, VPN-FW-6, VPN-FW-8

**Procedure Description:**

1) For each Inner VPN Gateway within the solution (hereafter referred to as Inner VPN Gateway A):

   a) For each other Inner VPN Gateway within the solution that protects a Red network of the same security level:

      i) Attempt to establish an IPsec VPN connection to it from Inner VPN Gateway A.

      ii) Verify that the VPN connection was established. (VPN-FW-1, VPN-FW-6)

   b) For each Inner VPN Gateway within the solution that protects a Red network of a different security level (hereafter referred to as Inner VPN Gateway B):

      i) Identify the first Gray Network Firewall on the physical path from Inner VPN Gateway A and Inner VPN Gateway B. If no such Firewall exist, skip the remainder of Step 1(b).

      ii) Place a packet sniffer on the interface of the Gray Network Firewall facing Inner VPN Gateway B.

      iii) Attempt to establish an IPsec VPN connection from Inner VPN Gateway A to Inner VPN Gateway B.

      iv) Verify that the VPN connection was not established.

v) Verify that the packet sniffer did not record any IKE or IPsec packets with a source address of Inner VPN Gateway A and a destination address of Inner VPN Gateway B. (VPN-FW-8)

vi) Verify that the Gray Network Firewall logs contain an event for an IKE or IPsec packet with a source address of Inner VPN Gateway A and a destination address of Inner VPN Gateway B. (VPN-AU-10)

**Expected Result:**

In Step 1(a), the Gray Network Firewall allows IKE and IPsec traffic between pairs of Inner VPN Gateways that are allowed to establish VPN tunnels with one another. In Step 1(b), the Gray Network Firewall denies IKE and IPsec traffic between pairs of Inner VPN Gateways that protect Red networks of different classification levels.

## 14.14 Gray Network Firewall HTTP Filtering Rules

This section contains a procedure for ensuring that the filtering rules on Gray Network Firewalls are configured so that the only HTTP traffic allowed through the firewall is from an Inner VPN Gateway to an Inner CDP.

**Requirements being tested:** VPN-AU-10, VPN-FW-2, VPN-FW-8

**Procedure Description:**

1) For each Inner VPN Gateway within the solution:

   a) For each Inner CDP within the solution:

      i) Attempt to have the Inner VPN Gateway download the current CRL from an Inner CDP.

      ii) Verify that the download was successful. (VPN-FW-2)

      iii) Identify the first Gray Network Firewall on the physical path from the Inner VPN Gateway to the Inner CDP. If no such Gray Network Firewall exists, skip the remainder of Step 1(a).

      iv) Place a packet sniffer on the interface of the Gray Network Firewall facing the Inner VPN Gateway.

      v) From the Inner CDP, attempt to make an HTTP request to the Inner VPN Gateway.

      vi) Verify that the request failed.

      vii) Verify that the packet sniffer did not record any packets with a source address of the Inner CDP and a destination address of the Inner VPN Gateway. (VPN-FW-8)

viii) Verify that the Gray Network Firewall logs contain an event for a packet with a source address of the Inner CDP and a destination address of the Inner VPN Gateway. (VPN-AU-10)

b) For every other device on the Gray network that is not an Inner CDP:

i) Identify the first Gray Network Firewall on the physical path from the Inner VPN Gateway to the other device. If no such Gray Network Firewall exists, skip the remainder of Step 1(b).

ii) Place a packet sniffer to the interface of the Gray Network Firewall facing the other device.

iii) Attempt to have the Inner VPN Gateway download a CRL from the other device.

iv) Verify that the download failed.

v) Verify that the packet sniffer did not record any packets with a source address of the Inner VPN Gateway and a destination address of the other device. (VPN-FW-8)

vi) Verify that the Gray Network Firewall logs contain an event for a packet with a source address of the Inner VPN Gateway and a destination address of the other device. (VPN-AU-10)

**Expected Results:**

In Step 1(a), the Gray Network Firewall allows HTTP requests from the Inner VPN Gateway to the Inner CDP, but not from the Inner CDP to the Inner VPN Gateway. In Step 1(b), the Gray Network Firewall denies HTTP requests from the Inner VPN Gateway to devices that are not Inner CDPs.

## 14.15 Gray Network Firewall Management

This section contains a procedure for ensuring that Gray Network Firewalls can only be managed from the Administration Workstation on the Gray Management network.

**Requirements being tested:** VPN-AU-10, VPN-FW-5

**Procedure Description:**

1) For each Gray Network Firewall within the solution:

a) From the Administration Workstation on the Gray Management network, attempt to connect to the Gray Network Firewall's remote management interface.

b) Verify that the connection attempt was successful. (VPN-FW-5)

c) For each physical network interface on the Gray Network Firewall except the one through which the Administration Workstation connects:

i) From a device reachable from the physical network interface, attempt to connect to the Gray Network Firewall's remote management interface.

ii) Verify that the connection attempt failed. (VPN-FW-5)

iii) Verify that the Gray Network Firewall logs contain an event for a packet with a source address of the selected device and a destination address of the Gray Network Firewall. (VPN-AU-10)

**Expected Results:**

In Step 1(b), the Gray Network Firewall allows management traffic from the Administration Workstation. In Step 1(c), the Gray Network Firewall blocks attempts to access the management interface through other physical network interfaces.

### 14.16 Gray Network Firewall Address Spoofing

This section contains a procedure for ensuring that Gray Network Firewalls detect spoofing of source addresses in traffic sent through it.

**Requirements being tested:** VPN-AU-10, VPN-FW-7

**Procedure Description:**

1) For each Gray Network Firewall within the solution:

   a) For each physical network interface on the Gray Network Firewall:

      i) Select a device on the network connected to that interface of the Gray Network Firewall. Hereafter the device will be called Device A.

      ii) Select a device on the network connected to an interface of the Gray Network Firewall that Device A is not connected to. Hereafter the device will be called Device B.

      iii) Select a device on the network connected to an interface of the Gray Network Firewall that Device A is not connected to, and that Device B is allowed to communicate with. Hereafter the device will be called Device C.

      iv) Place a network sniffer between the Gray Network Firewall and Device C.

      v) Configure Device A to use the IP address of Device B.

      vi) Attempt to send traffic from Device A (spoofing Device B's IP address) to Device C, of a type that Device B is allowed to send to Device C.

vii) Verify that the packet sniffer did not observe any packets with a source address of Device B and a destination address of Device C. (VPN-FW-7)

viii) Verify that the Gray Network Firewall logs contain an event for a packet received on the physical interface through which Device A connects, with a source address of Device B and a destination address of Device C. (VPN-AU-10)

**Expected Results:**

Each Gray Network Firewall detects the use of spoofed addresses and does not allow packets with spoofed source addresses from passing through, even if non-spoofed traffic from that source address would be allowed.

## 14.17 Gray Network Firewall HTTP Deep Packet Inspection

This section contains a procedure for ensuring that the deep packet inspection performed by the Gray Network Firewalls is configured so only the specific types of HTTP traffic desired between Inner VPN Gateways and Inner CDPs is allowed.

**Requirements being tested:** VPN-AU-10, VPN-FW-3, VPN-FW-4, VPN-FW-8

**Procedure Description:**

1) For each Inner VPN Gateway within the solution:

   a) For each Inner CDP within the solution:

      i) Attempt to have the Inner VPN Gateway download the current CRL from the Inner CDP.

      ii) Verify that the download was successful. (VPN-FW-3, VPN-FW-4)

      iii) Identify the first Gray Network Firewall on the physical path from the Inner VPN Gateway to the Inner CDP. If no such Gray Network Firewall exists, skip the remainder of Step 1(a).

      iv) Replace the CRL on the Inner CDP with a text file.

      v) Place a packet sniffer on the interface of the Gray Network Firewall facing the Inner VPN Gateway.

      vi) Attempt to have the Inner VPN Gateway download the current CRL from the Inner CDP.

      vii) Verify that the request failed.

      viii) Verify that the packet sniffer did not record any packets with a source address of the Inner CDP and a destination address of the Inner VPN Gateway that contains an HTTP response payload. (VPN-FW-4)

ix) Verify that the Gray Network Firewall logs contain an event for an improper HTTP response payload with a source address of the Inner CDP and a destination address of the Inner VPN Gateway. (VPN-AU-10)

x) Restore the CRL on the Inner CDP.

xi) Move the packet sniffer to the interface of the Gray Network Firewall facing the Inner CDP.

xii) Attempt to have the Inner VPN Gateway download a CRL from the Inner CDP using an incorrect URL.

xiii) Verify that the request failed.

xiv) Verify that the packet sniffer did not record any packets with a source address of the Inner VPN Gateway and a destination address of the Inner CDP. (VPN-FW-3)

xv) Verify that the Gray Network Firewall logs contain an event for an improper HTTP request with a source address of the Inner VPN Gateway and a destination address of the Inner CDP. (VPN-AU-10)

xvi) Attempt to have the Inner VPN Gateway issue an HTTP POST request for the URL of the CRL on the Inner CDP.

xvii) Verify that the request failed.

xviii) Verify that the packet sniffer did not record any packets with a source address of the Inner VPN Gateway and a destination address of the Inner CDP. (VPN-FW-3)

xix) Verify that the Gray Network Firewall logs contain an event for an improper HTTP request with a source address of the Inner VPN Gateway and a destination address of the Inner CDP. (VPN-AU-10)

b) For every other device on the Gray network that is not an Inner CDP, follow the procedure for Step 1(b) in Section 14.16. (VPN-AU-10, VPN-FW-8)

**Expected Results:**

In Step 1(a), the Gray Network Firewall allows only HTTP traffic between the Inner VPN Gateway and Inner CDP that consists of a GET request for the appropriate CRL and a response containing the CRL. In Step 1(b), the Gray Network Firewall denies HTTP requests from the Inner VPN Gateway to devices that are not Inner CDPs.

## 14.18 CRL CONFIGURATION FOR CDPS

This section contains procedures to ensure that the CRL configurations for the CDPs used within the VPN solution follow the requirements given in this Capability Package.

**Requirements being tested**: VPN-AU-20 through VPN-AU-22, VPN-CD-1 through VPN-CD-16

**Procedure Description:**

1) Verify that the CRL hosted by the Outer CDP does not contain extensions other than those specified in IETF RFC 5280. (VPN-CD-1)
   a) Pull down a valid CRL from the Gray Network CA.
   b) Verify that the CRL does not contain any fields that are not specified in IETF RFC 5280.
2) Verify that the CRL hosted on the Inner CDP is signed by the Red Network CA. (VPN-CD-2, VPN-CD-11)
   a) Download the CRL from the Inner CDP.
   b) Verify that the CRL is signed by the Red Network CA.
3) Verify that the CRL hosted on the Outer CDP is signed by the Gray Network CA. (VPN-CD-3, VPN-CD-12)
   a) Download the CRL from the Outer CDP.
   b) Verify that the CRL is signed by the Gray Network CA.
4) Verify that the Inner and Outer CDPs are only issuing CRLs over port 80. (VPN-CD-4)
   a) Perform a port scan on the Inner and Outer CDP and verify that the only open ports are 80 and the port used for management of the devices.
5) Verify that the implementing organization's policy describes an approved one way mechanism for transferring CRLs from the Red Network CA to the Inner CDP Server. (VPN-CD-5)
6) Verify that the implementing organization's policy describes an approved one way mechanism for transferring CRLs from the Gray Network CA to the Outer CDP Server. (VPN-CD-6)
7) Verify that the implementing organization has an approved policy in place that states a new CRL shall be transferred to a CDP server at least 4 days prior to the expiration of the current CRL and who will perform this action. (VPN-CD-7)

8) Verify that the VPN Gateway has checked the age of the current cached CRL prior to an establishment of a new connection. (VPN-CD-8)

   a) Log into the VPN Gateway and verify that it is configured to check the age of the current cached CRL prior to establishment of a new connection.

   b) Load a CRL with an age of greater than 1 hour onto a VPN Gateway.

   c) Attempt to establish a new connection between sites.

   d) Verify that the VPN Gateway checks the age of the current cached CRL.

9) Verify that the CDP only allows outbound traffic on port 80 and ports used for remote management traffic that adheres to VPN-DM-8. (VPN-CD-9)

   a) Log into the CDP and verify that it is configured to only allow outbound traffic on port 80 and ports used for remote management traffic in accordance with VPN-DM-8.

10) Verify that traffic filtering rules on the Inner and Outer CDPs are applied based on known VPN Gateway addresses. (VPN-CD-10)

   a) Remove a valid VPN Gateway from the whitelist.

   b) Have the removed VPN Gateway attempt to download the CRL from the CDP.

   c) Verify that the download fails.

11) Verify that the current CRL cached is used if integrity check of the CRL pulled from the CDP fails. (VPN-CD-13)

   a) Working with two Inner VPN Gateways (Gateway A and B) with valid certificates, load a valid CRL that will soon expire onto both Gateway A and B.

   b) Revoke the certificate for Gateway B.

   c) Issue a new CRL.

   d) Modify the CRL file.

   e) Load the modified CRL file on the CDP.

   f) Have Gateway A connect to Gateway B.

   g) Verify that the connection was successful.

h) Review the Gateway audit logs to verify that the modified CRL was downloaded and a validity check occurred and failed.

12) Verify that the implementing organization has an approved policy in place that states that the VPN Gateway is manually updated prior to the expiration of the current CRL if the CDP is down or contains a bad CRL. (VPN-CD-14)

13) Verify that the Red Network CA has set the CRL Distribution Points extension of certificates it generates to the list of URLs hosted by Inner CDPs. (VPN-CD-15)

a) Pull down a valid CRL from the Red Network CA.

b) Verify that the certificate extension for the CRL Distribution Points is set to the URLs hosted by the Inner CDPs.

14) Verify that the Gray Network CA has set the CRL Distribution Points extension of certificates it generates to the list of URLs hosted by Outer CDPs. (VPN-CD-16)

a) Pull down a valid CRL from the Gray Network CA.

b) Verify that the certificate extension for the CRL Distribution Points is set to the URLs hosted by the Outer CDPs.

15) Verify that the VPN Gateways log the failure to pull the CRL from the Inner or Outer CDP. (VPN-AU-20)

a) CDP Servers shall remove all CRLs.

b) VPN Gateways shall attempt to pull the CRL from their respective CDPs.

c) Review the VPN Gateways audit logs to verify that a log report is generated from failure to pull the CRL.

16) Verify that the VPN Gateways log if the version of the CRL on the Inner or Outer CDP is older than the current cached CRL. (VPN-AU-21)

a) Load the CDPs with CRLs that are older than the current cached CRLs on the VPN Gateways.

b) Have the VPN Gateways attempt to pull the CRLs.

c) Review the VPN Gateway audit logs to verify that a log report is generated.

17) Verify that the VPN Gateways log if signature validation of the CRL on the Inner or Outer CDP fails. (VPN-AU-22)

a) Load the CDPs with CRLs that contain an invalid signature.

b) Have the VPN Gateways pull the CRLs.

c) Review the VPN Gateway audit logs to verify that a log report is generated due to an invalid CRL signature.

**Expected Results:**

For Step 1, the CRL should only contain fields specified in IETF RFC 5280. For Steps 2-3, the CRL hosted on the Inner and Outer CDP shall be signed by the Red Network CA and Gray Network CA respectively. For Step 4, the Inner and Outer CDP CRL's should only be issued on port 80. For Steps 5-7 & 13, the implementing organization should have policies in place to address the requirements identified. For Steps 8-9, the VPN Gateway should retrieve a new CDP CRL. For Step 10, the CDP will only allow outbound traffic on port 80 and ports used for remote management traffic. For Step 11, the VPN Gateway's attempt to download a CRL should fail. For step 12, the current CRL cached should be used. For Steps 13-14, the Red and Gray CAs shall have the certificate extension for the CRL Distribution Points set to the URLs hosted by the Inner CDP and Outer CDP respectively. For Steps 15-17, there should be an audit log entry created for each requirement.

## 14.19 Incident Reporting Guidance

This section ensures that procedures are followed regarding incident reporting to NSA in the event a solution owner identifies a security incident which affects the solution.

**Requirements being tested**: VPN-RP-1 through VPN-RP-12

**Procedure Description:**

1) Verify the procedures given in VPN-RP-1 through VPN-RP-12 were/are followed and are currently in place.

**Expected Results:**

For Step 1 all of these procedures have been followed or are in place.

# APPENDIX A. GLOSSARY OF TERMS

**Accreditation** – The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST 800-37)

**Assurance** – Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. (CNSSI 4009)

**Audit** – The activity of monitoring the operation of a product from within the product. It includes monitoring of a product for a set of pre-determined events. Each audit event may indicate rogue behavior, or a condition that is detrimental to security, or provide necessary forensics to identify the source of rogue behavior.

**Audit Log** – A chronological record of the audit events that have been deemed critical to security. The audit log can be used to identify potentially malicious activity that may further identify the source of an attack, as well as potential vulnerabilities where additional countermeasures or corrective actions are required.

**Availability** – Assurance that the system and its associated assets are accessible and protected against Denial of Service attacks, as well as available when the user needs them and in the form needed by the user.

**Black Box Testing** – Testing the functionality of a component of the solution, such that testing is limited to the subset of functionality that is available from the external interfaces of the box during its normal operational configuration without any additional privileges (such as given to the Security Administrator or Auditor).

**Black Network** – A network that contains classified data that has been encrypted twice. (See Section 4.1.1)

**Capability Package** – The set of guidance provided by NSA that describes recommended approaches to composing COTS components to protect classified information for a particular class of security problem. This package will point to potential products that can be used as part of this solution.

**Central Management Site** – A site within a VPN solution that is responsible for remotely managing the solution components located at other sites. (See Section 4.3.1.2)

**Certification** – The technical evaluation of a system's security features, performed as a part of and in support of the approval/accreditation process that establishes the extent to which a particular computer system's design and implementation meet a set of specified security requirements.

**Certification and Accreditation (C&A)** – A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. In conjunction with the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST 800-37).

**Certificate Authority (CA)** – An authority trusted by one or more users to create and assign certificates. [ISO9594-8]

**Certificate Policy (CP)** – A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. [IETF RFC 3647]

**Committee on National Security Systems Policy No. 15 (CNSSP-15)** – Policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS).

**Confidentiality** – Assurance that the data stored in, processed by, or transmitted by the system are protected against unauthorized disclosure, and confidence that only the appropriate set of individuals or organizations would be provided the information.

**Control Plane Protocol** – A routing, signaling, or similar protocol whose endpoints are network infrastructure devices such as VPN Gateways or routers. Control plane protocols carry neither user data nor management traffic.

**CRL Distribution Point (CDP)** – A web server that hosts a copy of a CRL issued by a CA for VPN Gateways to download. (See Section 5.7)

**Cross Domain Solution (CDS)** – A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains. [CNSSI 4009]

**Data Plane Protocol** – A protocol that carries the data being transferred through the solution.

**Designated Approving Authority (DAA)** – The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk, synonymous with designating accrediting authority and delegated accrediting authority. [CNSSI 4009]

**External Interface** – The interface on a VPN Gateway that connects to the outer network (i.e., the Gray network on the Inner VPN Gateway or the Black network on the Outer VPN Gateway).

**Federal Information Processing Standards (FIPS)** – A set of standards that describe the handling and processing of information within governmental agencies.

**Gray Box Testing** – The ability to test functionality within a component of the solution, such that full management privileges are granted (i.e., knowing passwords for security administrator and Auditor and access to the capabilities associated with those privileges). In addition, the use of any and all testing equipment and/or testing software used inside and outside the developed solution is available.

**Gray Network** – A network that contains classified data that has been encrypted once. (See Section 4.1.1)

**Gray Network Firewall** – A stateful traffic filtering firewall placed on the Gray network to provide additional separation between flows of singly-encrypted data of different classification levels. (See Section 5.5)

**Independently Managed Site** – A site within a VPN solution whose solution components are locally managed and that does not remotely manage other sites' solution components. (See Section 4.3.1.1)

**Internal Interface** – The interface on a VPN Gateway that connects to the inner network (i.e., the Gray network on the Outer VPN Gateway or the Red network on the Inner VPN Gateway).

**Locally Managed Device** – A device that is being managed by the direct connection of the Administration Workstation to the device in a hardwired fashion (such as a console cable).

**Malicious** – Any unauthorized events that are either unexplained or in any way indicate adversary activity.

**Management Plane Protocol** – A protocol that carries either traffic between a system administrator and a component being managed, or log messages from a solution component to a log server or similar repository.

**Protection Profile** – A document used as part of the certification process according to the Common Criteria. As the generic form of a security target, it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements.

**Public Key Infrastructure (PKI)** – Framework established to issue, maintain, and revoke public key certificates.

**Red Network** – A network that contains unencrypted classified data. (See Section 4.1.1)

**Remotely Managed Device** – A device that is being managed by any other method besides that given in the definition of a Locally Managed Device.

**Remote Site** – A site within a VPN solution whose solution components are remotely managed by a Central Management Site. (See Section 4.3.1.2)

**Security Level** – The combination of classification level, list of compartments, dissemination controls, and other controls applied to the information within a network.

**VPN Gateway** – The term used to refer to VPN Gateways and VPN Clients.

**VPN Gateway** – A VPN device physically located within the VPN infrastructure.

**VPN Infrastructure** – Physically protected in a secure facility and includes Inner and Outer VPN Gateways, Certificate Authorities, and Administration Workstations, but does not include s.

## APPENDIX B. ACRONYMS

| Acronym | Definition |
|---|---|
| AES | Advanced Encryption Standard |
| AIS | Automated Information System |
| AO | Authorizing Official |
| ARP | Address Resolution Protocol |
| BFD | Bidirectional Forwarding Detection |
| BIOS | Basic Input/Output System |
| C&A | Certification and Accreditation |
| CA | Certificate Authority |
| CAA | Certificate Authority Administrator |
| CDP | CRL Distribution Point |
| CDS | Cross Domain Solution |
| CNSS | Committee on National Security Systems |
| CNSSI | Committee on National Security Systems Instruction |
| CNSSP | Committee on National Security Systems Policy |
| COTS | Commercial Off-the-Shelf |
| CP | Certificate Policy |
| CP | Capability Package |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| CSfC | Commercial Solutions for Classified |
| CUI | Controlled Unclassified Information |
| DAA | Designated Approving Authority |
| DAR | Data-at-Rest |
| DDoS | Distributed Denial of Service |
| DH | Diffie Hellman |
| DHCP | Dynamic Host Configuration Protocol |
| DISA | Defense Information Systems Agency |
| DM | Device Management |
| DNS | Domain Name System |
| DoS | Denial of Service |
| DSA | Digital Signature Algorithm |
| ECDH | Elliptic Curve Diffie Hellman |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| ESP | Encapsulating Security Payload |
| FDE | Full Disk Encryption |
| FIPS | Federal Information Processing Standards |
| GOTS | Government Off-the-Shelf |
| GRE | Generic Routing Encapsulation |
| HTTP | Hypertext Transfer Protocol |

| Acronym | Definition |
|---|---|
| HTTPS | Hypertext Transfer Protocol Secure |
| IAD | Information Assurance Directorate |
| IAVA | Information Assurance Vulnerability Alerts |
| ICMP | Internet Control Message Protocol |
| ICT | Information Communication Technology |
| IDS | Intrusion Detection System |
| IETF | Internet Engineering Task Force |
| IGMP | Internet Group Management Protocol |
| IKE | Internet Key Exchange |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| IPsec | Internet Protocol Security |
| IPv4 | Internet Protocol Version 4 |
| IPv6 | Internet Protocol Version 6 |
| KM | Key Management |
| MLD | Multicast Listener Discovery |
| MTU | Maximum Transmission Unit |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| NSS | National Security Systems |
| NTP | Network Time Protocol |
| O | Objective |
| O&M | Operation and Maintenance |
| OID | Object Identifier |
| OPSEC | Operational Security |
| OS | Operating System |
| OSPF | Open Shortest Path First |
| PKI | Public Key Infrastructure |
| PMTU | Path Maximum Transmission Unit |
| RFC | Request for Comment |
| RSA | Rivest Shamir Adelman algorithm |
| S3 | Secure Sharing Suite |
| SA | Security Association |
| SCRM | Supply Chain Risk Management |
| SHA | Secure Hash Algorithm |
| SIPRNet | Secret Internet Protocol Router Network |
| SP | Service Packs |
| SSH | Secure Shell |
| SSHv2 | Secure Shell Version 2 |
| T | Threshold |
| T&E | Test and Evaluation |
| TCP | Transmission Control Protocol |

| Acronym | Definition |
|---|---|
| TLS | Transport Layer Security |
| UDP | User Datagram Protocol |
| UML | Unified Markup Language |
| VM | Virtual Machine |
| VPN | Virtual Private Network |

## APPENDIX C. REFERENCES


| | | |
|---|---|---|
| CNSSI 1300 | *CNSSI 1300, National Security Systems Public Key Infrastructure X.509 Certificate Policy* | October 2009 |
| CNSSI 4009 | *CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems.* http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf | April 2010 |
| CNSSP 11 | *CNSS Policy (CNSSP) Number 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products.* | June 2013 |
| CNSSP 15 | *CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems* | March 2010 |
| CNSSD 505 | *CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)* | March 2012 |
| FIPS 140 | *Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf | May 2001 |
| FIPS 180 | *Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)* | March 2012 |
| FIPS 186 | *Federal Information Processing Standard 186-4, Digital Signature Standard (DSS)* | July 2013 |
| FIPS 197 | *Federal Information Processing Standard 197, Advanced Encryption Standard (AES)* | November 2001 |
| FIPS 201 | *Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf | March 2006 |
| IPsec VPN Client PP | *Protection Profile for IPsec Virtual Private Network (VPN) Clients*. http://www.niap-ccevs.org/pp | January 2012 |
| NSA Suite B | *NSA Guidance on Suite B Cryptography [including the Secure Sharing Suite (S3)]*. http://www.nsa.gov/ia/programs/ suiteb_cryptography/index.shtml | November 2010 |
| RFC 2409 | *IETF RFC 2409 The Internet Key Exchange (IKE)*. D. Harkins and D. Carrel. | November 1998 |
| RFC 3647 | *IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* Internet Engineering Task Force | November 2003 |
| RFC 4252 | *IETF RFC 4252 The Secure Shell (SSH) Authentication Protocol*. T. Ylonen and C. Lonvick. | January 2006 |

| | | |
|---|---|---|
| RFC 4253 | *IETF RFC 4253 The Secure Shell (SSH) Transport Layer Protocol*. T. Ylonen and C. Lonvick. | January 2006 |
| RFC 4254 | *IETF RFC 4254 The Secure Shell (SSH) Connection Protocol*. T. Ylonen and C. Lonvick. | January 2006 |
| RFC 4256 | *IETF RFC 4256 Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)*. F. Cusack and M. Forssen. | January 2006 |
| RFC 4302 | *IETF RFC 4302 IP Authentication Header*. S. Kent | December 2005 |
| RFC 4303 | *IETF RFC 4303 IP Encapsulating Security Payload*. S. Kent | December 2005 |
| RFC 4307 | *IETF RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*. J. Schiller | December 2005 |
| RFC 4308 | *IETF RFC 4308 Cryptographic Suites for IPsec*. P. Hoffman | December 2005 |
| RFC 4754 | *IETF RFC 4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*. D. Fu and J. Solinas. | January 2007 |
| RFC 5246 | *IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2*. T. Dierks and E. Rescorla. | August 2008 |
| RFC 5280 | *IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. D. Cooper, et. al. | May 2008 |
| RFC 5759 | *IETF RFC 5759 Suite B Certificate and Certificate Revocation List (CRL) Profile*. J. Solinas and L. Zieglar. | January 2010 |
| RFC 5996 | *IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)*. C. Kaufman, et. al. | September 2010 |
| RFC 6239 | *IETF RFC 6239 Suite B Cryptographic Suites for Secure Shell (SSH)*. K. Igoe. | May 2011 |
| RFC 6379 | *IETF RFC 6379 Suite B Cryptographic Suites for IPsec*. L. Law and J. Solinas. | October 2011 |
| RFC 6380 | *IETF RFC 6380 Suite B Profile for Internet Protocol Security (IPsec)*. K. Burgin and M. Peck. | October 2011 |
| RFC 6460 | *IETF RFC 6460 Suite B Profile for Transport Layer Security (TLS)*. M. Salter and R. Housley. | January 2012 |
| RFC 6818 | *IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. P. Yee | January 2013 |
| RFC 7030 | *IETF RFC 7030 Enrollment over Secure Transport*. M. Pritikin, P. Yee, and D. Harkins. | October 2013 |
| SP 800-53 | *NIST Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations*. Joint Task Force Transformation Initiative. | April 2013 |

| | | |
|---|---|---|
| SP 800-56A | *NIST Special Publication 800-56A Rev. 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. E. Barker, et. al. | May 2013 |
| SP 800-56B | *NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*. E. Barker, et. al. | August 2009 |
| SP 800-56C | *NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion*. L. Chen. | November 2011 |
| SP 800-131A | *NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths*. E. Barker. | January 2011 |
| SP 800-147 | *NIST Special Publication 800-147, BIOS Protection Guidelines*. D. Cooper, et. al. | April 2011 |

# APPENDIX D. SUMMARY OF CHANGES TO REQUIREMENTS

This appendix summarizes the changes between the requirements in this Capability Package and the requirements in its predecessor, the CSfC VPN Capability Package version 2.0, dated May 28, 2013. It is provided as an aide to solution owners who have developed a solution compliant with the earlier Capability Package and wish to determine the extent to which their existing solution complies with this Capability Package.

In general, requirements included in the CSfC VPN Capability Package version 2.0, dated May 28, 2013, are also included in this Capability Package without any substantive changes. The wording used in several requirements has been changed to clarify their intent, and typically a solution that complied with their original wording is expected to also comply with their revised wording.

Most of the new requirements added in this Capability Package only apply to the two new optional capabilities introduced in this Capability Package, described in Sections 4.3.3.2 and 4.3.4. The primary exceptions to this are, but are not limited to, the following:

- New requirements addressing the content and distribution of CRLs (see Section 10.10.1)
- New port filtering requirements (see Section 10.6)
- New device management requirements (see Section 10.8)
- New incident reporting requirements (see Section 11.2)

Table 24 lists in detail each requirement from the CSfC VPN Capability Package version 2.0 that has changed in this Capability Package, except for changes that are purely cosmetic and do not affect the content of the requirement. Table 24 also identifies requirements that have been withdrawn or superseded by other requirements. Any requirements not listed here have not changed.

**Table 22. Changes to VPN CP 3.1 Requirements**

| VPN CP 3.1 Requirement | Change Description |
|---|---|
| VPN-PS-2 | Removed. |
| VPN-PS-9 | Removed. |
| VPN-PS-11 | Removed. |
| VPN-PS-18 | Removed. |
| VPN-SR-1 | Removed. |
| VPN-SR-6 | Removed. |
| VPN-CR-2 | Removed. |
| VPN-CR-9 | Removed. |
| VPN-CR-13 | Removed. |

| VPN CP 3.1 Requirement | Change Description |
|---|---|
| VPN-CR-14 | Removed. |
| VPN-CR-24 | Removed. |
| VPN-IR-4 | Removed. |
| VPN-OR-4 | Removed. |
| VPN-OR-5 | Removed. |
| VPN-OR-6 | Removed. |
| VPN-EU-1 | Removed. |
| VPN-EU-2 | Removed. |
| VPN-EU-3 | Removed. |
| VPN-EU-4 | Removed. |
| VPN-EU-5 | Removed. |
| VPN-EU-6 | Removed. |
| VPN-EU-7 | Removed. |
| VPN-EU-8 | Removed. |
| VPN-EU-9 | Removed. |
| VPN-EU-10 | Removed. |
| VPN-EU-11 | Removed. |
| VPN-OR-12 | Removed. |
| VPN-OR-13 | Removed. |
| VPN-EU-14 | Removed. |
| VPN-EU-15 | Removed. |
| VPN-EU-16 | Removed. |
| VPN-EU-17 | Removed. |
| VPN-EU-18 | Removed. |
| VPN-EU- 19 | Removed. |
| VPN-EU-20 | Removed. |
| VPN-PF-4 | Removed. |
| VPN-PF-5 | Removed. |
| VPN-RA-1 | Removed. |
| VPN-RA-2 | Removed. |
| VPN-RA-3 | Removed. |
| VPN-RA-4 | Removed. |
| VPN-RA-5 | Removed. |
| VPN-RA-6 | Removed. |
| VPN-RA-7 | Removed. |
| VPN-RA-8 | Removed. |
| VPN-RA-9 | Removed. |
| VPN-AU-13 | Removed. |
| VPN-AU-21 | Removed. |
| VPN-AU-22 | Removed. |
| VPN-AU-23 | Removed. |
| VPN-AU-24 | Removed. |

| VPN CP 3.1 Requirement | Change Description |
|---|---|
| VPN-AU-25 | Removed. |
| VPN-AU-29 | Removed. |
| VPN-AU-30 | Removed. |
| VPN-AU-43 | Removed. |
| VPN-KM-13 | Removed. |
| VPN-GD-2 | Removed. |
| VPN-GD-4 | Removed. |
| VPN-GD-6 | Removed. |
| VPN-GD-7 | Removed. |
| VPN-GD-8 | Removed. |
| VPN-GD-27 | Removed. |
| VPN-GD-38 | Removed. |
| VPN-RP-10 | Removed. |
| VPN-GD-32 | Removed. |
| VPN-GD-33 | Removed. |
| VPN-GD-34 | Removed. |
| VPN-GD-35 | Removed. |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

# APPENDIX E. MAPPINGS TO NIST SP 800-53 CONTROLS

Most of the requirements in this Capability Package support the implementation of security controls specified in NIST SP 800-53 Revision 4. This appendix is provided for customers who must demonstrate implementation of a set of NIST SP 800-53 security controls as part of their C&A process for a system incorporating a VPN solution that complies with this Capability Package.

Note that the presence of a mapping between a requirement and a NIST SP 800-53 security control does not necessarily indicate that the requirement is by itself sufficient to fully address the security control. Instead, it indicates that implementation of the requirement provides some degree of support to implementation of the security control. Additional work outside the scope of this Capability Package may be needed for the overall system to implement the security control.

**Table 23. Mappings to NIST SP 800-53 Security Controls**

| Requirement | NIST SP 800-53 Revision 4 Security Controls |
|---|---|
| VPN-PS-1 | SA-4(6B/7A+B) |
| VPN-PS-2 | SA-4(6B/7A+B) |
| VPN-PS-3 | SA-4(6B/7A+B) |
| VPN-PS-4 | SA-12(13) |
| VPN-PS-5 | SA-12, SA-4(6A+B) |
| VPN-PS-6 | SC-3(1/5) |
| VPN-PS-7 | SC-3(2/3) |
| VPN-PS-8 | SA-12(13) |
| VPN-PS-9 | SA-12(13) |
| VPN-PS-10 | SA-12(13) |
| VPN-PS-11 | SA-12(13) |
| VPN-PS-12 | SA-12(13) |
| VPN-PS-13 | SA-4(6/7), SA-12/13, SA-9(1A) |
| VPN-PS-14 | SA-3(5) |
| VPN-PS-15 | SA-3(5) |
| VPN-PS-16 | SC-3(1) |
| VPN-PS-17 | SC-3(1) |
| VPN-PS-18 | SA-3(5) |
| VPN-SR-1 | *Withdrawn* |
| VPN-SR-2 | SC-3(2) |
| VPN-SR-3 | None |
| VPN-SR-4 | AU-8(1B) |
| VPN-SR-5 | AU-8(1B) |
| VPN-SR-6 | None |
| VPN-SR-7 | AC-2(1), IA-5(1/5/E), SA-4(5) |
| VPN-SR-8 | CM-2, CM-6(4), CM-9 |

| Requirement | NIST SP 800-53 Revision 4 Security Controls |
|---|---|
| VPN-CR-1 | SC-12(2/3), SC-13 |
| VPN-CR-2 | *Withdrawn* |
| VPN-CR-3 | IA-3(2), IA-4(D), IA-5(5/E/H/G), AC-16 |
| VPN-CR-4 | IA-3(2), IA-4(D), IA-5(5/E/H/G) |
| VPN-CR-5 | AU-10, SC-23(5), SC-17 |
| VPN-CR-6 | SC-12(2/3), IA-3(1/4) |
| VPN-CR-7 | IA-5(2) |
| VPN-CR-8 | IA-5(2) |
| VPN-CR-9 | *Withdrawn* |
| VPN-CR-10 | SC-31, SC-32, AC-4, CA-3(1/2), SC-3(2), SC-7(10/21) |
| VPN-CR-11 | None |
| VPN-CR-12 | None |
| VPN-CR-13 | *Withdrawn* |
| VPN-CR-14 | *Withdrawn* |
| VPN-CR-15 | CA-3(2) |
| VPN-CR-16 | CA-3(2) |
| VPN-CR-17 | CA-3(6), SC-8(1/3) |
| VPN-CR-18 | SC-12 |
| VPN-CR-19 | SC-12 |
| VPN-CR-20 | SC-12 |
| VPN-CR-21 | IA-5(10/F) |
| VPN-CR-22 | IA-5(10/F) |
| VPN-CR-23 | IR-9, PE-19, SC-7(14/22) |
| VPN-CR-24 | IR-9, PE-19, SC-7(14/22) |
| VPN-CR-25 | IA-3(1/4) |
| VPN-IR-1 | SC-7, AC-4 |
| VPN-IR-2 | SC-8(3) |
| VPN-IR-3 | IA-7, SC-11/13, SC-8(1/2) |
| VPN-IR-4 | IA-7, SC-11/13, SC-8(1/2) |
| VPN-IR-5 | IA-7, SC-11/13, SC-8(1/2) |
| VPN-OR-1 | SC-7, AC-4 |
| VPN-OR-2 | IA-7, SC-11/13, SC-8(1/2) |
| VPN-OR-3 | IA-7, SC-11/13, SC-8(1/2) |
| VPN-OR-4 | IA-7, SC-11/13, SC-8(1/2) |
| VPN-OR-5 | *Withdrawn* |
| VPN-OR-6 | SC-3(3), AC-6 |
| VPN-OR-7 | IA-7, SC-11/13 SC-8(1/2) |
| VPN-PF-1 | AC-4, SC-7 |
| VPN-PF-2 | AC-4, SC-7 |
| VPN-PF-3 | AC-4, SC-7 |
| VPN-PF-4 | AC-4, SC-7 |
| VPN-PF-5 | AC-4, SC-7 |

| Requirement | NIST SP 800-53 Revision 4 Security Controls |
|---|---|
| VPN-PF-6 | AC-4, SC-7, PL-9, AC-19, CM-7, SI-2, AC-3 MA-1, MP-7 |
| VPN-PF-7 | AC-4, SC-7, PL-9, AC-19, CM-7, SI-2, AC-3, MA-1, MP-7 |
| VPN-PF-8 | CM-7(1/2/3/4/5) |
| VPN-PF-9 | CM-7(1/3) |
| VPN-PF-10 | None |
| VPN-PF-11 | CM-7(1/2/3/4/5) |
| VPN-PF-12 | CM-7(1/2/3/4/5) |
| VPN-PF-13 | AC-4(21), CA-3(2), SC-3 |
| VPN-PF-14 | AC-4(21), CA-3(2), SC-3 |
| VPN-PF-15 | AC-4(21), CA-3(2), SC-3 |
| VPN-PF-16 | AC-4(21), CA-3(2), SC-3 |
| VPN-PF-17 | AC-4(21), CA-3(2), SC-3 |
| VPN-PF-18 | AC-4(21), CA-3(2), SC-3 |
| VPN-PF-19 | AC-4 SC-7 |
| VPN-PF-20 | CA-3(5/I) |
| VPN-CM-1 | CM-2, CA-1 |
| VPN-CM-2 | CM-3(5), AU-3 |
| VPN-CM-3 | CM-3(5), AU-3 |
| VPN-DM-1 | SC-32 |
| VPN-DM-2 | SC-32 |
| VPN-DM-3 | AC-4(2) |
| VPN-DM-4 | SC-8(1), SC-11 |
| VPN-DM-5 | SC-8(1), SC-11 |
| VPN-DM-6 | SC-32 |
| VPN-DM-7 | CM-2, CM-6 |
| VPN-DM-8 | AC-2(7) |
| VPN-DM-9 | SC-12, SC-13 |
| VPN-DM-10 | SC-12, SC-13 |
| VPN-DM-11 | SC-13 |
| VPN-DM-12 | CM-6, SC-7(4A/5/18), SC-17, MP-6(A+B/1) |
| VPN-DM-13 | SC-12, SC-13, SC-17,SC-23(5) |
| VPN-DM-14 | SC-17 |
| VPN-DM-15 | SC-17 |
| VPN-DM-16 | SC-32 |
| VPN-DM-17 | AU-1/2/3 |
| VPN-DM-18 | AU-1/2/3 |
| VPN-DM-19 | SC-7(21) |
| VPN-DM-20 | SC-7(21) |
| VPN-DM-21 | PS-3(1/2) |
| VPN-AU-1 | AU-1/2/3/14 |
| VPN-AU-2 | AU-1/2/3/14 |
| VPN-AU-3 | AU-1/2/3/14 |

| Requirement | NIST SP 800-53 Revision 4 Security Controls |
|---|---|
| VPN-AU-4 | AU-1/2/3/14 |
| VPN-AU-5 | AU-1/2/3/14 |
| VPN-AU-6 | AU-1/2/3/14 |
| VPN-AU-7 | AU-1/2/3/14 |
| VPN-AU-8 | AU-1/2/3/14 |
| VPN-AU-9 | AU-1/2/3/14 |
| VPN-AU-10 | AU-1/2/3/14 |
| VPN-AU-11 | AU-1/2/3/14 |
| VPN-AU-12 | AU-1/2/3/14 |
| VPN-AU-13 | *Withdrawn* |
| VPN-AU-14 | AU-1/2/3/14 |
| VPN-AU-15 | AU-1/2/3/14 |
| VPN-AU-16 | AU-1/2/3/14 |
| VPN-AU-17 | AU-1/2/3/14 |
| VPN-AU-18 | AU-1/2/3/14 |
| VPN-AU-19 | AU-1/2/3/14 |
| VPN-AU-20 | AU-1/2/3/14 |
| VPN-AU-21 | AU-1/2/3/6/14 |
| VPN-AU-22 | AU-1/2/3/6/14, IR-4, IA-5(2/D) |
| VPN-AU-23 | AU-1/2/3/14 IR-4 |
| VPN-AU-26 | AU-1/2/3/14 |
| VPN-AU-27 | AU-1/2/3/14 |
| VPN-AU-28 | AU-1/2/3/14 |
| VPN-AU-29 | AU-1/2/3/14 |
| VPN-AU-30 | AU-1/2/3/14 |
| VPN-AU-31 | AU-13(1) |
| VPN-AU-32 | AU-6 CM-6 |
| VPN-AU-33 | AU-6 CM-6 |
| VPN-AU-34 | AC-4(1) |
| VPN-AU-35 | AC-4(1) |
| VPN-AU-36 | AU-5(2) |
| VPN-AU-37 | AU-2/3/ |
| VPN-AU-38 | AU-2/3/ |
| VPN-AU-39 | AU-2/3/ |
| VPN-AU-40 | AU-1/2/3 |
| VPN-AU-41 | CM-2(2) SC-2 |
| VPN-AU-42 | PE-3(5), SA-18(1)(2) |
| VPN-AU-43 | PE-3(5), SA-18(1)(2) |
| VPN-KM-1 | SC-12(2/3), SC-13 |
| VPN-KM-2 | SC-3(1) |
| VPN-KM-3 | SC-12 |
| VPN-KM-4 | SC-12(2/3), SC-13 |

| Requirement | NIST SP 800-53 Revision 4 Security Controls |
|---|---|
| VPN-KM-5 | SC-12(2/3), SC-13 |
| VPN-KM-6 | SC-13(4) |
| VPN-KM-7 | SA-13 |
| VPN-KM-8 | SA-13 |
| VPN-KM-9 | IA-2/3/7, SC-12/13 |
| VPN-KM-10 | CP-2(4/5), SC-12(1) |
| VPN-KM-11 | CA-3(2) |
| VPN-KM-12 | SC-12(1) IA-5(13) |
| VPN-KM-14 | CA-3(2), SC-12(1), IA-5(13) |
| VPN-KM-15 | IA-5(14) CM-8(7) |
| VPN-KM-16 | SC-12 |
| VPN-KM-17 | IA-4 |
| VPN-KM-18 | SC-23(5), PL-1, RA-1 |
| VPN-KM-19 | IA-5(2) |
| VPN-KM-20 | IA-4 |
| VPN-KM-21 | CM-7 |
| VPN-KM-22 | CM-7 |
| VPN-KM-23 | CM-7 |
| VPN-KM-24 | IA-3/4 |
| VPN-KM-25 | IA-5(2/D) |
| VPN-KM-26 | IA-5(2/D) |
| VPN-KM-27 | IA-5(2/D) |
| VPN-KM-28 | IA-5(2/D) |
| VPN-FW-1 | AC-4(21), CA-3(2), SC-3 |
| VPN-FW-2 | AC-4(21), CA-3(2), SC-3 |
| VPN-FW-3 | AC-4(21), CA-3(2), SC-3 |
| VPN-FW-4 | AC-4(21), CA-3(2), SC-3 |
| VPN-FW-5 | CA-3, MA-1, AC-4(21), MA-4(4), SC-3 |
| VPN-FW-6 | AC-4(21), CA-3(2), SC-3 |
| VPN-FW-7 | AC-4(21), CA-3(2/5), SC-3 |
| VPN-FW-8 | CA-3(5/I) |
| VPN-SR-9 | AC-4(21), CA-3(2), SC-3 |
| VPN-SR-10 | AC-4(21), CA-3(2) SC-3 |
| VPN-CD-1 | CM-7 |
| VPN-CD-2 | AU-10 |
| VPN-CD-3 | AU-10 |
| VPN-CD-4 | CM-7 |
| VPN-CD-5 | CM-7 |
| VPN-CD-6 | CM-7 |
| VPN-CD-7 | IA-5(2) |
| VPN-CD-8 | IA-5(2) |
| VPN-CD-9 | IA-5(2) |

| Requirement | NIST SP 800-53 Revision 4 Security Controls |
|---|---|
| VPN-CD-10 | CM-7 |
| VPN-CD-11 | CM-7 |
| VPN-CD-12 | CM-7 |
| VPN-CD-13 | SC-16(1) |
| VPN-CD-14 | IA-5(2/D), IR-4(3) |
| VPN-CD-15 | SC-3(4) |
| VPN-CD-16 | SC-3(4) |
| VPN-GD-1 | PE-1/3 |
| VPN-GD-2 | PE-1/3 |
| VPN-GD-3 | PE-1/3 |
| VPN-GD-4 | PE-1/3 |
| VPN-GD-5 | SA-19(3), MP-6 |
| VPN-GD-6 | SA-19(3), MP-6 |
| VPN-GD-7 | SA-19(3), MP-6 |
| VPN-GD-8 | AC-3(8) |
| VPN-GD-9 | SA-12(1) |
| VPN-GD-10 | SA-12(15), AU-1, AU-16(2) |
| VPN-GD-11 | AU-1 |
| VPN-GD-12 | AU-1 |
| VPN-GD-13 | AU-1 |
| VPN-GD-14 | CM-2(1) |
| VPN-GD-15 | AU-1 |
| VPN-GD-16 | AU-4 |
| VPN-GD-17 | AU-4(1) |
| VPN-GD-18 | AU-9 |
| VPN-GD-19 | AU-1/4/5 |
| VPN-GD-20 | AU-1/5 AU-4(1) |
| VPN-GD-21 | AU-1/4/5 |
| VPN-GD-22 | AU-1/4/5 |
| VPN-GD-23 | IA-5, IA-5(4) |
| VPN-GD-24 | SI-2 |
| VPN-GD-25 | SI-2 |
| VPN-GD-26 | PE-19(1) |
| VPN-GD-27 | AC-3(9) |
| VPN-GD-28 | PS-2 |
| VPN-GD-29 | PS-1 |
| VPN-GD-30 | PS-2, PM-13/14 |
| VPN-GD-31 | SC-3(5), SA-8, SA-4(6) |
| VPN-GD-32 | SI-1, PM-15, IR-1/4 |
| VPN-GD-33 | AC-3(8) |
| VPN-GD-34 | *Withdrawn* |
| VPN-GD-35 | SC-4/28 |

| Requirement | NIST SP 800-53 Revision 4 Security Controls |
|---|---|
| VPN-GD-36 | CM-2/1, CM-4/2 |
| VPN-GD-37 | CM-8/1/4 |
| VPN-GD-38 | AC-18 |
| VPN-GD-39 | AC-5 |
| VPN-RP-1 | IR-6/1/2 |
| VPN-RP-2 | IR-6/1 |
| VPN-RP-3 | IR-6/1/2 |
| VPN-RP-4 | IR-6/1/2 |
| VPN-RP-5 | IR-6/1/2 |
| VPN-RP-6 | IR-6/1/2 |
| VPN-RP-7 | IR-6/1/2 |
| VPN-RP-8 | IR-6/1/2 |
| VPN-RP-9 | IR-6/1/2 |
| VPN-RP-10 | IR-6/1/2 |
| VPN-RP-11 | IR-6/1/2 |
| VPN-RP-12 | IR-6/1/2 |
| VPN-RP-13 | IR-6/1/2 |
| VPN-RP-14 | IR-6/1/2 |
| VPN-TR-1 | CA-2(1) |